# Diseño de la redes de vSAN

Update 3

VMware vSphere 7.0
VMware vSAN 7.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

**VMware, Inc.**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

**VMware Spain, S.L.**
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

# Contenido

# Acerca del diseño de redes vSAN

1

En la guía de *diseño de redes devSAN* se describen los requisitos y el diseño de las redes, así como las prácticas de configuración para implementar un clúster de vSAN con un alto nivel de disponibilidad y escalabilidad.

vSAN es una solución de almacenamiento distribuido. Al igual que con cualquier solución distribuida, la red es un componente importante del diseño. Para obtener los mejores resultados, debe seguir las instrucciones proporcionadas en este documento porque un diseño o un hardware de red incorrecto pueden provocar resultados negativos.

En VMware, valoramos la inclusión. Para fomentar este principio de forma interna y en nuestra comunidad de clientes y socios, creamos contenido con un lenguaje inclusivo.

## Audiencia prevista

Esta guía está destinada a cualquier usuario que diseñe, implemente y administre un clúster de vSAN. La información de esta guía está escrita para administradores de red con experiencia que estén familiarizados con el diseño y la configuración de redes, la administración de máquinas virtuales y las operaciones de centros de datos virtuales. En este manual, se asume que estos usuarios están familiarizados con VMware vSphere, incluidos VMware ESXi, vCenter Server y vSphere Client.

## Documentos relacionados

Además de esta guía, puede consultar las siguientes guías para obtener más información sobre las redes de vSAN:

- *Guía de planificación e implementación de vSAN*, para obtener más información sobre la creación de clústeres de vSAN
- *Administrar VMware vSAN*, para configurar un clúster de vSAN y obtener más información sobre las funciones de vSAN
- *Guía de supervisión y solución de problemas de vSAN*, para supervisar y solucionar problemas de los clústeres de vSAN

# Información actualizada

2

Este documento se actualiza con cada versión del producto o cuando sea necesario.

Esta tabla brinda información sobre el historial de actualizaciones del documento *Diseño de las redes de vSAN*.

| Revisión | Descripción |
| --- | --- |
| 12 de junio de 2023 | Se actualizaron Ejemplo de configuración de Network I/O Control y vSphere RDMA. |
| 6 de octubre de 2020 | Versión inicial. |

# Introducción a la red de vSAN

3

Puede usar vSAN para aprovisionar el almacenamiento compartido dentro de vSphere. vSAN agrega dispositivos de almacenamiento locales o con conexión directa de un clúster de host y crea un grupo de almacenamiento individual compartido entre todos los hosts del clúster de vSAN.

vSAN es una solución de almacenamiento distribuida y compartida que depende de una red bien configurada y de alta disponibilidad para el tráfico de almacenamiento de vSAN. Una red con un alto nivel de rendimiento y disponibilidad es crucial para una implementación correcta de vSAN. Esta guía proporciona recomendaciones sobre cómo diseñar y configurar una red de vSAN.

vSAN tiene una arquitectura distribuida basada en una red de alto rendimiento, escalable y resistente. Todos los nodos del host de un clúster de vSAN se comunican a través de la red IP. Los hosts deben mantener la conectividad de unidifusión IP para que puedan comunicarse a través de una red de capa 2 o capa 3. Para obtener más información sobre la comunicación de unidifusión, consulte Capítulo 5 Usar la unidifusión en redes de vSAN.

Las versiones anteriores a la versión 6.6 de vSAN requieren multidifusión de IP. Si es posible, utilice siempre la versión más reciente de vSAN. Para obtener más información sobre la multidifusión, consulte Capítulo 14 Usar la multidifusión en la red de vSAN.

Este capítulo incluye los siguientes temas:



## Términos y definiciones de redes de vSAN

vSAN introduce términos y definiciones específicos que resulta importante comprender. Antes de comenzar a diseñar su red de vSAN, revise los términos y definiciones clave de vSAN.

### CLOM

El administrador de objetos en el nivel del clúster (CLOM) es responsable de garantizar que la configuración de un objeto coincida con su directiva de almacenamiento. El CLOM comprueba si hay suficientes grupos de discos disponibles para satisfacer esa directiva. Decide dónde colocar los testigos y los componentes en un clúster.

## CMMDS

La supervisión, pertenencia y servicio de directorio de del clúster (CMMDS) es responsable de la recuperación y el mantenimiento de un clúster de miembros del nodo de red. Administra el inventario de elementos, como nodos de host, dispositivos y redes. También almacena información de metadatos, como las políticas y la configuración de RAID para los objetos de vSAN.

## DOM

El administrador de objetos distribuidos (DOM) es responsable de crear los componentes y distribuirlos en todo el clúster. Después de crear un objeto DOM, uno de los nodos (host) se designa como el propietario del DOM para ese objeto. Este host controla todas las IOPS de ese objeto DOM mediante la ubicación de los componentes secundarios correspondientes en el clúster y el redireccionamiento de las operaciones de E/S a los respectivos componentes a través de la red de vSAN. Los objetos DOM incluyen vDisk, Snapshot, vmnamespace, vmswap, vmem, etc.

## LSOM

El administrador de objetos con estructura de registros (LSOM) es responsable de almacenar localmente los datos en el sistema de archivos vSAN como componente u objeto LSOM de vSAN (componente de datos o testigo).

## Formación de equipos de NIC

La formación de equipos de la tarjeta de interfaz de red (NIC) puede definirse como dos o más adaptadores de red (NIC) configurados como "equipo" para un alto nivel de disponibilidad y equilibrio de carga.

## NIOC

Network I/O Control (NIOC) determina el ancho de banda que se otorga a diferentes tipos de tráfico de red en vSphere Distributed Switch. La distribución del ancho de banda es un parámetro configurable por el usuario. Cuando NIOC está habilitado, el tráfico del conmutador distribuido se divide en grupos de recursos de red predefinidos: tráfico de tolerancia a errores, tráfico de iSCSI, tráfico de vMotion, tráfico de administración, tráfico de vSphere Replication, tráfico de NFS y tráfico de máquina virtual.

## Objetos y componentes

Cada objeto consta de un conjunto de componentes, determinado por las funcionalidades utilizadas en la directiva de almacenamiento de máquina virtual.

Un almacén de datos de vSAN contiene varios tipos de objeto.

**Espacio de nombres del directorio principal de la máquina virtual**

El espacio de nombres de inicio de la máquina virtual es un directorio principal de la máquina virtual en el que se almacenan todos los archivos configuración de máquina virtual. Esto incluye archivos como `.vmx`, archivos de registro, VMDK y archivos de descripción delta de instantánea.

**VMDK**

VMDK es un disco de máquina virtual o un archivo `.vmdk` que almacena el contenido de la unidad de disco duro de la máquina virtual.

**Objeto de intercambio de máquina virtual**

Los objetos de intercambio de máquina virtual se crean cuando se enciende una máquina virtual.

**VMDK delta de instantáneas**

Los VMDK delta de instantánea se crean cuando se toman instantáneas de la máquina virtual.

**Objeto de memoria**

Los objeto de memoria se crean cuando está seleccionada la opción de memoria de instantánea al crear o suspender una máquina virtual.

## RDT

El protocolo de transporte de datos fiable (RDT) se utiliza para la comunicación entre hosts a través de los puertos de VMkernel de vSAN. Utiliza TCP en la capa de transporte y es responsable de crear y destruir las conexiones TCP (sockets) a petición. Está optimizado para enviar archivos de gran tamaño.

## SPBM

La administración de almacenamiento basada en directivas (SPBM) proporciona un marco de directivas de almacenamiento que sirve como un panel de control unificado para un amplio rango de servicios de datos y soluciones de almacenamiento. Este marco le ayuda a alinear el almacenamiento con las demandas de aplicación de sus máquinas virtuales.

## VASA

Las API de almacenamiento de vSphere para reconocimiento de almacenamiento (VASA) es un conjunto de interfaces de programación de aplicaciones (API) que permite a vCenter Server reconocer las capacidades de las matrices de almacenamiento. Los proveedores de VASA se comunican con vCenter Server para determinar la topología de almacenamiento, la capacidad y la información de estado que admite la administración basada en directivas, la administración de operaciones y la funcionalidad de DRS.

## VLAN

Una VLAN permite que se segmente un único segmento LAN físico para que los grupos de puertos queden aislados unos de otros como si estuvieran en segmentos físicamente diferentes.

## Componente testigo

Un testigo es un componente que contiene únicamente metadatos y no datos reales de aplicaciones. Sirve como factor determinante cuando se debe tomar una decisión en relación con la disponibilidad de los componentes del almacén de datos restantes después de un error potencial. Un testigo utiliza aproximadamente 2 MB de espacio para metadatos en el almacén de datos de vSAN cuando se utiliza el formato en disco 1.0, y consume 4 MB para el formato en disco de la versión 2.0 y versiones posteriores.

# Información sobre las redes de vSAN

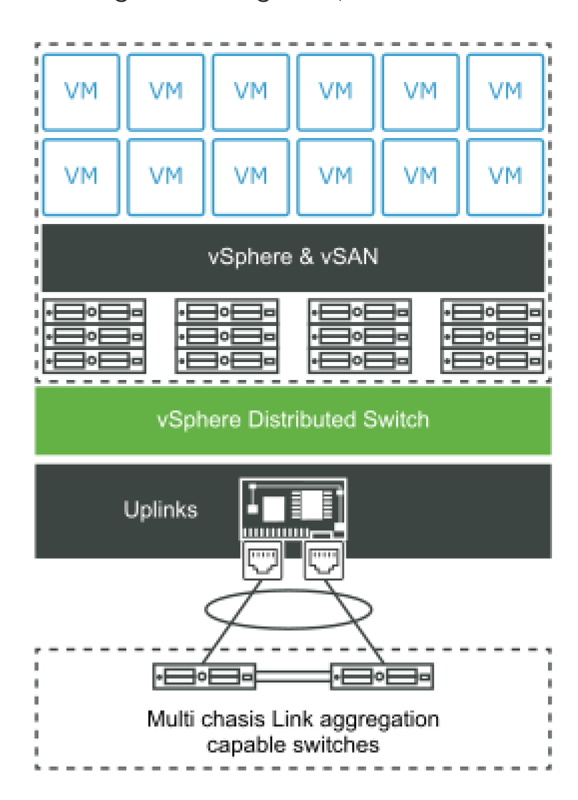
4

Una red de vSAN facilita la comunicación entre los hosts del clúster y debe garantizar un rendimiento rápido, una alta disponibilidad y ancho de banda.

vSAN utiliza la red para comunicarse entre los hosts ESXi y para la E/S de disco de la máquina virtual.

Las máquinas virtuales de almacenes de datos de vSAN se componen de un conjunto de objetos, y cada uno de ellos puede estar compuesto por uno o varios componentes. Estos componentes se distribuyen entre varios hosts para obtener resistencia ante errores de host y de unidad. vSAN mantiene y actualiza estos componentes mediante la red de vSAN.

En el siguiente diagrama, se ofrece una descripción general de alto nivel de la red de vSAN:




Este capítulo incluye los siguientes temas:

- Características de red de vSAN
- Tipos de tráfico de ESXi

- Requisitos de red para vSAN

# Características de red de vSAN

vSAN depende de la red. Conocer y configurar los ajustes adecuados para la red de vSAN es esencial para evitar problemas de rendimiento y estabilidad.

Una red de vSAN sólida y fiable debe tener las siguientes características:

**Unidifusión**

vSAN 6.6 y las versiones posteriores admiten la comunicación de unidifusión. El tráfico de unidifusión es una transmisión de paquetes de IP desde un punto de la red a otro. La unidifusión transmite el latido enviado desde el host principal al resto de hosts cada segundo. Eso garantiza que los hosts estén activos e indica la participación de los hosts en el clúster de vSAN. Es posible designar una red de unidifusión simple para vSAN. Para obtener más información sobre la comunicación de unidifusión, consulte Capítulo 5 Usar la unidifusión en redes de vSAN.

**Multidifusión**

Las versiones anteriores a vSAN 6.6 usan la comunicación de multidifusión IP como protocolo de detección para identificar los nodos que intentan unirse a un clúster de vSAN.

---

**Nota** Si es posible, utilice siempre la versión más reciente de vSAN.

---

La multidifusión IP se basa en los protocolos de comunicación que utilizan los hosts, los clientes y los dispositivos de red para participar en las comunicaciones basadas en multidifusión. Para obtener más información sobre la comunicación de multidifusión, consulte Capítulo 14 Usar la multidifusión en la red de vSAN.

**Redes de capa 2 y capa 3**

Todos los hosts del clúster de vSAN deben estar conectados a través de una red de capa 2 o capa 3. Las versiones de vSAN anteriores a vSAN 6.0 solo admiten redes de capa 2, mientras que las versiones posteriores admiten los protocolos de capa 2 y capa 3. Utilice una red de capa 2 o capa 3 para permitir la comunicación entre los sitios de datos y el sitio testigo. Para obtener más información sobre las topologías de red de capa 2 y capa 3, consulte Implementaciones estándar.

**Red de VMkernel**

Cada host ESXi de un clúster de vSAN debe tener un adaptador de red para la comunicación de vSAN. Todas las comunicaciones del nodo dentro del clúster se producen a través del puerto de VMkernel de vSAN. Los puertos de VMkernel proporcionan servicios de capa 2 y capa 3 a cada host vSAN y a las máquinas virtuales alojadas.

**Tráfico de redes de vSAN**

Hay disponibles varios tipos de tráfico diferentes en la red de vSAN, como el tráfico de almacenamiento y el tráfico de unidifusión. El proceso y almacenamiento de una máquina virtual pueden estar en el mismo host o en hosts diferentes del clúster. Una máquina virtual que no está configurada para tolerar un error puede ejecutarse en un host y acceder a un componente o un objeto de máquina virtual que reside en un host diferente. Esto implica que todas las operaciones de E/S de la máquina virtual pasarán a través de la red. El tráfico de almacenamiento constituye la mayor parte del tráfico en un clúster de vSAN.

La comunicación relacionada con el clúster entre todos los hosts ESXi crea tráfico en el clúster de vSAN. Este tráfico de unidifusión también contribuye al tráfico de red de vSAN.

**Conmutador virtual**

vSAN admite los siguientes tipos de conmutadores virtuales:

- El conmutador virtual estándar proporciona la conectividad de las máquinas virtuales y los puertos de VMkernel a las redes externas. Este conmutador es local para cada host ESXi.
- vSphere Distributed Switch proporciona un control central de la administración del conmutador virtual en varios hosts ESXi. Los conmutadores distribuidos también proporcionan funciones de red, como Network I/O Control (NIOC), que pueden ayudarle a establecer niveles de calidad de servicio (QoS) en vSphere o en la red virtual. vSAN incluye vSphere Distributed Switch independientemente de la versión de vCenter Server.

**Ancho de banda**

El tráfico de vSAN puede compartir adaptadores de red físicos de 10 GbE, 25 GbE, 40 GbE y 100 GbE con otros tipos de tráfico del sistema, como el tráfico de vSphere vMotion, el tráfico de vSphere HA y el tráfico de la máquina virtual. También proporciona más ancho de banda para las configuraciones de red compartidas donde vSAN, la administración de vSphere, el tráfico de vSphere vMotion, etc., se encuentran en la misma red física. Para garantizar la cantidad de ancho de banda necesaria para vSAN, use vSphere Network I/O Control en el conmutador distribuido.

En vSphere Network I/O Control, puede configurar la reserva y los recursos compartidos para el tráfico saliente de vSAN:

- Configure una reserva para que Network I/O Control garantice que un ancho de banda mínimo esté disponible en el adaptador físico para vSAN.
- Configure el valor de recursos compartidos en 100 de modo que, cuando se sature el adaptador físico para vSAN, haya un cierto ancho de banda disponible para vSAN. Por ejemplo, es posible que el adaptador físico se sature cuando se produce un error en otro adaptador físico del equipo y todo el tráfico del grupo de puertos se transfiere a los demás adaptadores del equipo.

Para obtener más información sobre cómo utilizar Network I/O Control para configurar la asignación de ancho de banda para el tráfico de vSAN, consulte el documento *Redes de vSphere*.

# Tipos de tráfico de ESXi

Los hosts de ESXi utilizan diferentes tipos de tráfico de red para admitir vSAN.

A continuación, se indican los diferentes tipos de tráfico que debe configurar para vSAN.

**Tabla 4-1. Tipos de tráfico de red**

| Tipos de tráfico | Descripción |
| --- | --- |
| Red de administración | La red de administración es la interfaz de red principal que utiliza una pila de TCP/IP de VMkernel para facilitar la administración y la conectividad del host. También puede controlar el tráfico del sistema, como vMotion, iSCSI, Network File System (NFS), canal de fibra sobre Ethernet (FCoE) y tolerancia a errores. |
| Red de máquinas virtuales | Con las redes virtuales, puede crear máquinas virtuales de red y crear redes complejas dentro de un único host de ESXi o entre varios hosts de ESXi. |
| Red de vMotion | Tipo de tráfico que facilita la migración de la máquina virtual de un host a otro. La migración con vMotion requiere que las interfaces de red estén correctamente configuradas en los hosts de origen y destino. Asegúrese de que la red de vMotion sea distinta de la red de vSAN. |
| Red de vSAN | Un clúster de vSAN requiere la red de VMkernel para el intercambio de datos. Cada host ESXi del clúster de vSAN debe tener un adaptador de red de VMkernel para el tráfico de vSAN. Para obtener más información, consulte Configurar una red de VMkernel para vSAN. |

# Requisitos de red para vSAN

vSAN es una solución de almacenamiento distribuido que depende de la red para la comunicación entre hosts. Antes de su implementación, asegúrese de que el entorno de vSAN tenga todos los requisitos de red.

## Requisitos de NIC física

Las tarjetas de interfaz de red (NIC) que se utilizan en hosts vSAN deben cumplir ciertos requisitos. vSAN funciona en redes de 10 Gbps, 25 Gbps, 40 Gbps, 50 Gbps y 100 Gbps.

Las implementaciones de vSAN deben garantizar que se cumplan los requisitos mínimos de NIC.

Tabla 4-2. Recomendaciones y requisitos mínimos de NIC

| Topología o modo de implementación | Arquitectura | Compatibilidad con NIC de 1 GbE | Compatibilidad con NIC de 10 GbE | Compatibilidad con varias NIC de más de 10 GbE | Latencia entre nodos | Latencia o ancho de banda de vínculo entre sitios | Latencia entre nodos y hosts testigo de vSAN | Ancho de banda entre nodos y hosts testigo de vSAN |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Clúster estándar | Clúster híbrido | Sí (mínimo) | Sí (recomendado) | Sí | Menos de 1 ms de RTT. | No corresponde | No corresponde | No corresponde |
| | Clúster basado íntegramente en tecnología flash | No | Sí | Sí (recomendado) | | | | |
| Clúster ampliado | Clúster híbrido o basado íntegramente en tecnología Flash | No | Sí (mínimo) | Sí | Menos de 1 ms de RTT en cada sitio. | Se recomiendan 10 GbE (según la carga de trabajo) y 5 ms de RTT como máximo. | Menos de 200 ms de RTT. Hasta 10 hosts por sitio.<br>Menos de 100 ms de RTT. 11-15 hosts por sitio. | 2 Mbps por cada 1000 componentes (máximo de 100 Mbps con componentes de 45 k). |
| Clúster de dos hosts | Clúster híbrido | Sí (hasta 10 máquinas virtuales) | Sí (recomendado) | Sí | Menos de 1 ms de RTT dentro del mismo sitio. | Se recomiendan 10 GbE y 5 ms de RTT como máximo. | Menos de 500 ms de RTT. | 2 Mbps por cada 1000 componentes (máximo de 1,5 Mbps). |
| | Clúster basado íntegramente en tecnología flash | No | Sí (mínimo) | | | | | |

**Nota** Estos requisitos de NIC asumen que la pérdida de paquetes no es superior al 0,0001 % en entornos hiperconvergentes. Superar alguno de estos requisitos puede tener un impacto drástico en el rendimiento de vSAN.

Para obtener más información sobre los requisitos de NIC de clúster ampliado, consulte la *Guía de clúster ampliado de vSAN*.

## Requisitos de latencia y ancho de banda

Para garantizar un alto nivel de rendimiento y disponibilidad, los clústeres de vSAN deben cumplir ciertos requisitos de ancho de banda y latencia de red.

Los requisitos de ancho de banda entre los sitios principal y secundario de un clúster ampliado de vSAN dependen de la carga de trabajo de vSAN, de la cantidad de datos y de la forma en que se desea controlar los errores. Para obtener más información, consulte la *Guía de diseño y redimensionamiento de VMware vSAN*.

### Tabla 4-3. Requisitos de latencia y ancho de banda

| Comunicación de sitios | Ancho de banda | Latencia |
| --- | --- | --- |
| Sitio a sitio | Mínimo de 10 Gbps | Menos de 5 ms de RTT de latencia. |
| Sitio a testigo | 2 Mbps por 1000 componentes de vSAN | ■ Menos de 500 ms de RTT de latencia para 1 host por sitio.<br>■ Menos de 200 ms de RTT de latencia para hasta 10 hosts por sitio.<br>■ Menos de 100 ms de RTT de latencia para 11-15 hosts por sitio. |

## Compatibilidad con capa 2 y capa 3

VMware recomienda la conectividad de capa 2 entre todos los hosts vSAN que comparten la subred.

vSAN también admite implementaciones con conectividad enrutada de capa 3 entre hosts vSAN. Debe tener en cuenta el número de saltos y la latencia adicional que se producen mientras se enruta el tráfico.

### Tabla 4-4. Compatibilidad con capa 2 y capa 3

| Tipo de clúster | Admite capa 2 | Admite capa 3 | Consideraciones |
| --- | --- | --- | --- |
| Clúster híbrido | Sí | Sí | Se recomienda capa 2 y se admite capa 3. |
| Clúster basado íntegramente en tecnología flash | Sí | Sí | Se recomienda capa 2 y se admite capa 3. |
| Datos del clúster ampliado | Sí | Sí | Se admiten la capa 2 y la capa 3 entre los sitios de datos. |
| Testigo de clúster ampliado | No | Sí | Admite capa 3. No se admite la capa 2 entre sitios testigo y de datos. |
| Clúster de dos nodos | Sí | Sí | Se admiten la capa 2 y la capa 3 entre los sitios de datos. |

## Requisitos de enrutamiento y conmutación

Los tres sitios en un clúster ampliado se comunican en la red de administración y la red de vSAN. Las máquinas virtuales en todos los sitios de datos se comunican en una red de máquina virtual común.

A continuación se indican los requisitos de enrutamiento de clúster ampliado de vSAN:

**Tabla 4-5. Requisitos de enrutamiento**

| Comunicación de sitios | Modelo de implementación | Capa | Enrutamiento |
| --- | --- | --- | --- |
| Sitio a sitio | Predeterminado | Capa 2 | No es obligatorio |
| Sitio a sitio | Predeterminado | Capa 3 | Se requieren rutas estáticas. |
| Sitio a testigo | Predeterminado | Capa 3 | Se requieren rutas estáticas. |
| Sitio a testigo | Separación de tráfico testigo | Capa 3 | Las rutas estáticas son obligatorias cuando se utiliza una interfaz que no sea la de administración (vmk0). |
| Sitio a testigo | Separación de tráfico testigo | Capa 2 para clúster de dos hosts | No se requieren rutas estáticas. |

## Requisitos de conmutador virtual

Puede crear una red de vSAN con el conmutador estándar de vSphere o vSphere Distributed Switch. Utilice un conmutador distribuido para priorizar el ancho de banda para el tráfico de vSAN. vSAN utiliza un conmutador distribuido con todas las versiones de vCenter Server.

En la siguiente tabla se comparan las ventajas y los beneficios de un conmutador distribuido respecto a un conmutador estándar:

**Tabla 4-6. Tipos de conmutadores virtuales**

| Requisito de diseño | Opción 1: vSphere Distributed Switch | Opción 2: Conmutador estándar de vSphere | Descripción |
| --- | --- | --- | --- |
| Disponibilidad | Sin impacto | Sin impacto | Puede usar cualquiera de las opciones |
| Facilidad de administración | Impacto positivo | Impacto negativo | El conmutador distribuido se administra de forma centralizada en todos los hosts, a diferencia del conmutador estándar que se administra individualmente en cada host. |

Tabla 4-6. Tipos de conmutadores virtuales (continuación)

| Requisito de diseño | Opción 1: vSphere Distributed Switch | Opción 2: Conmutador estándar de vSphere | Descripción |
|---|---|---|---|
| Rendimiento | Impacto positivo | Impacto negativo | El conmutador distribuido incorpora controles, como Network I/O Control, que permite garantizar el rendimiento del tráfico de vSAN. |
| Recuperabilidad | Impacto positivo | Impacto negativo | Se puede realizar una copia de seguridad y restaurar la configuración del conmutador distribuido, mientras que el conmutador estándar no dispone de esta función. |
| Seguridad | Impacto positivo | Impacto negativo | El conmutador distribuido incorpora controles de seguridad integrados para ayudar a proteger el tráfico. |

# Requisitos del puerto de red de vSAN

Las implementaciones de vSAN requieren ajustes y puertos de red específicos para proporcionar acceso y servicios.

vSAN envía mensajes en ciertos puertos en cada host del clúster. Compruebe que los firewalls del host permitan el tráfico en estos puertos. Para obtener la lista de todos los puertos y protocolos compatibles de vSAN, consulte el portal VMware Ports and Protocols en https://ports.vmware.com/.

## Consideraciones de firewall

Cuando se habilita vSAN en un clúster, se agregan todos los puertos necesarios a reglas de firewall de ESXi y se configuran automáticamente. No es necesario que un administrador abra ningún puerto de firewall ni que habilite manualmente los servicios de firewall.

Puede ver los puertos abiertos para las conexiones entrantes y salientes. Seleccione el host ESXi y haga clic en **Configurar > Perfil de seguridad**.

# Requisitos del firewall de red

Cuando configure el firewall de red, tenga en cuenta la versión de vSAN que va a implementar.

Cuando se habilita vSAN en un clúster, se agregan todos los puertos necesarios a reglas de firewall de ESXi y se configuran automáticamente. No es necesario abrir ningún puerto de firewall ni habilitar manualmente los servicios de firewall. Puede ver los puertos abiertos para las conexiones entrantes y salientes en el perfil de seguridad del host ESXi (**Configurar > Perfil de seguridad**).

### Regla de firewall vsanEncryption

Si el clúster utiliza el cifrado vSAN, tenga en cuenta la comunicación entre los hosts y el servidor KMS .

El cifrado vSAN requiere un servidor de administración de claves (Key Management Server, KMS) externo. vCenter Server obtiene los identificadores de las claves del KMS y las distribuye entre los hosts ESXi. Los servidores KMS y los hosts ESXi se comunican directamente entre sí. Los servidores KMS pueden utilizar números de puerto diferentes, por lo que la regla de firewall vsanEncryption permite simplificar la comunicación entre cada host vSAN y el servidor KMS. Esto permite que un host vSAN se comunique directamente con cualquier puerto de un servidor KMS (puerto TCP 0 a 65535).

Cuando un host establece comunicación con un servidor KMS, se producen las siguientes operaciones.

- La dirección IP del servidor de KMS se agrega a la regla vsanEncryption y la regla de firewall se habilita.
- La comunicación entre el nodo de vSAN y el servidor KMS se establece durante el intercambio.
- Después de que la comunicación entre el nodo de vSAN y el servidor de KMS finaliza, la dirección IP se elimina de la regla vsanEncryptiony la regla de firewall se deshabilita de nuevo.

Los hosts de vSAN se pueden comunicar con varios hosts de KMS usando la misma regla.

# Usar la unidifusión en redes de vSAN

5

El tráfico de unidifusión hace referencia a una transmisión desde un punto de la red a otro. vSAN 6.6 y las versiones posteriores utilizan unidifusión para simplificar el diseño y la implementación de redes.

Todos los hosts ESXi utilizan el tráfico de unidifusión y vCenter Server se convierte en el origen de la pertenencia del clúster. Los nodos de vSAN se actualizan automáticamente con la lista de pertenencia al host más reciente que proporciona vCenter. vSAN se comunica mediante unidifusión para las actualizaciones de CMMDS.

Las versiones anteriores a vSAN 6.6 dependen de la multidifusión para habilitar el latido y para intercambiar metadatos entre los hosts del clúster. Si algunos hosts del clúster de vSAN ejecutan versiones anteriores del software, se requerirá una red de multidifusión. El conmutador a una red de unidifusión desde multidifusión proporciona un mejor rendimiento y compatibilidad de la red. Para obtener más información sobre la multidifusión, consulte Capítulo 14 Usar la multidifusión en la red de vSAN.

Este capítulo incluye los siguientes temas:



## Comportamiento de grupo de discos previo a la versión 5

La disponibilidad de un solo grupo de discos de versión 5 en un grupo de discos de vSAN 6.6 activa el clúster para comunicarse de forma permanente en el modo de unidifusión.

Los clústeres de vSAN 6.6 se revierten automáticamente a la comunicación de multidifusión en las siguientes situaciones:

- Todos los hosts del clúster ejecutan vSAN 6.5 o una versión anterior.
- Todos los grupos de discos utilizan la versión 3 del formato en disco o una versión anterior.

- Se agrega al clúster un host que no es de vSAN 6.6, como vSAN 6.2 o vSAN 6.5.

Por ejemplo, si se agrega un host que ejecuta vSAN 6.5 o una versión anterior a un clúster existente de vSAN 6.6, el clúster volverá al modo de multidifusión e incluirá el host 6.5 como nodo válido. Para evitar este comportamiento, utilice la versión más reciente tanto para los hosts ESXi como para el formato en disco. Para asegurarse de que el clúster de vSAN continúe comunicándose en modo de unidifusión y no revierta a multidifusión, actualice los grupos de discos de los hosts vSAN 6.6 a la versión de formato en disco 5.0.

**Nota** Evite tener un clúster de modo mixto donde vSAN 6.5 o versiones anteriores estén disponibles en el mismo clúster, junto con vSAN 6.6 o versiones posteriores.

## Comportamiento del grupo de discos de la versión 5

La presencia de un solo grupo de discos de versión 5 en un clúster de vSAN 6.6 activa el clúster para comunicarse de forma permanente en modo de unidifusión.

En un entorno en el que un clúster de vSAN 6.6 ya utiliza un formato en disco de versión 5 y se agrega un nodo de vSAN 6.5 al clúster, ocurre lo siguiente:

- El nodo de vSAN 6.5 crea su propia partición de red.
- El nodo de vSAN 6.5 sigue comunicándose en el modo de multidifusión, pero no puede comunicarse con los nodos de vSAN 6.6 cuando usan el modo de unidifusión.

Aparece una advertencia de resumen del clúster en el formato en disco que muestra que un nodo se encuentra en una versión anterior. Puede actualizar el nodo a la versión más reciente. No se pueden actualizar las versiones de formato de disco cuando un clúster está en modo mixto.

## Compatibilidad con DHCP en una red de unidifusión

vCenter Server implementadas en un clúster de vSAN 6.6 pueden utilizar direcciones IP del protocolo de configuración dinámica de host (DHCP) sin reservas.

Puede usar DHCP con reservas, ya que las direcciones IP asignadas se vinculan con las direcciones MAC de los puertos de VMkernel.

## Compatibilidad con IPv6 en red de unidifusión

vSAN 6.6 admite IPv6 con comunicaciones de unidifusión.

Con IPv6, la dirección local de vínculo se configura automáticamente en cualquier interfaz mediante el prefijo local de vínculo. De forma predeterminada, vSAN no agrega la dirección local de vínculo de un nodo a otros nodos de clústeres vecinos. Como resultado, vSAN 6.6 no admite las direcciones locales de vínculo IPv6 para las comunicaciones de unidifusión.

# Consultar unidifusión con ESXCLI

Puede ejecutar comandos de ESXCLI para determinar la configuración de unidifusión.

## Ver los modos de comunicación

Mediante el comando `esxcli vsan cluster get`, puede ver el modo CMMDS (unidifusión o multidifusión) del nodo del clúster de vSAN.

### Procedimiento

- Ejecute el comando `esxcli vsan cluster get`.

### Resultados

```
Cluster Information
  Enabled: true
  Current Local Time: 2020-04-09T18:19:52Z
  Local Node UUID: 5e8e3dc3-43ab-5452-795b-a03d6f88f022
  Local Node Type: NORMAL
  Local Node State: AGENT
  Local Node Health State: HEALTHY
  Sub-Cluster Master UUID: 5e8e3d3f-3015-9075-49b6-a03d6f88d426
  Sub-Cluster Backup UUID: 5e8e3daf-e5e0-ddb6-a523-a03d6f88dd4a
  Sub-Cluster UUID: 5282f9f3-d892-3748-de48-e2408dc34f72
  Sub-Cluster Membership Entry Revision: 11
  Sub_cluster Member Count: 5
  Sub-Cluster Member UUIDs: 5e8e3d3f-3015-9075-49b6-a03d6f88d426, 5e8e3daf-e5e0-ddb6-a523-
a03d6f88dd4a,
  5e8e3d73-6d1c-0b81-1305-a03d6f888d22, 5e8e3d33-5825-ee5c-013c-a03d6f88ea4c,
5e8e3dc3-43ab-5452-795b-a03d6f88f022
  Sub-Cluster Member HostNames: testbed-1.vmware.com, testbed2.vmware.com,
  testbed3.vmware.com, testbed4.vmware.com, testbed5.vmware.com
  Sub-Cluster Membership UUID: 0f438e5e-d400-1bb2-f4d1-a03d6f88d426
  Modo de unidifusión habilitado: true
  Maintenance Mode State: OFF
  Config Generation: ed845022-5c08-48d0-aa1d-6b62c0022222 7 2020-04-08T22:44:14.889
```

## Verificar hosts de clúster

Utilice el comando `esxcli vsan cluster unicastagent list` para comprobar si los hosts del clúster de vSAN funcionan en modo de unidifusión.

### Procedimiento

- Ejecute el comando `esxcli vsan cluster unicastagent list`.

### Resultados

```
NodeUuid                             IsWitness Supports Unicast IP Address  Port  Iface Name
Cert Thumbprint  SubClusterUuid
------------------------------------ --------- ---------------- ----------  ----- ----------
5e8e3d73-6d1c-0b81-1305-a03d6f888d22         0      true
```

```
10.198.95.10    12321
43:80:B7:A1:3F:D1:64:07:8C:58:01:2B:CE:A2:F5:DE:D6:B1:41:AB
5e8e3daf-e5e0-ddb6-a523-a03d6f88dd4a         0      true
10.198.94.240   12321
FE:39:D7:A5:EF:80:D6:41:CD:13:70:BD:88:2D:38:6C:A0:1D:36:69
5e8e3d3f-3015-9075-49b6-a03d6f88d426         0      true
10.198.94.244   12321
72:A3:80:36:F7:5D:8F:CE:B0:26:02:96:00:23:7D:8E:C5:8C:0B:E1
5e8e3d33-5825-ee5c-013c-a03d6f88ea4c         0      true
10.198.95.11    12321
5A:55:74:E8:5F:40:2F:2B:09:B5:42:29:FF:1C:95:41:AB:28:E0:57
```

El resultado incluye el UUID del nodo de vSAN, la dirección IPv4, la dirección IPv6, el puerto UDP con el que se comunica el nodo vSAN y si el nodo es un host de datos (0) o un host testigo (1). Puede utilizar este resultado para identificar los nodos del clúster de vSAN que funcionan en modo de unidifusión y ver el resto de hosts del clúster. vCenter Server mantendrá la lista de resultados.

## Consultar la información de la red

Utilice el comando `esxcli vsan network list` para ver la información de la red de vSAN, como la interfaz de VMkernel que utiliza vSAN para la comunicación, el puerto de unidifusión (12321) y el tipo de tráfico (vSAN o testigo) asociado con la interfaz de vSAN.

### Procedimiento

- Ejecute el comando `esxcli vsan network list`.

### Resultados

```
Interface
  VmkNic Name: vmk1
  IP Protocol: IP
  Interface UUID: e290be58-15fe-61e5-1043-246e962c24d0
  Agent Group Multicast Address: 224.2.3.4
  Agent Group IPv6 Multicast Address: ff19::2:3:4
  Agent Group Multicast Port: 23451
  Master Group Multicast Address: 224.1.2.3
  Master Group IPv6 Multicast Address: ff19::1:2:3
  Master Group Multicast Port: 12345
  Puerto de enlace del canal de unidifusión del host: 12321
  Multicast TTL: 5
  Traffic Type: vsan
```

Este resultado también muestra la información de multidifusión.

# Tráfico dentro del clúster

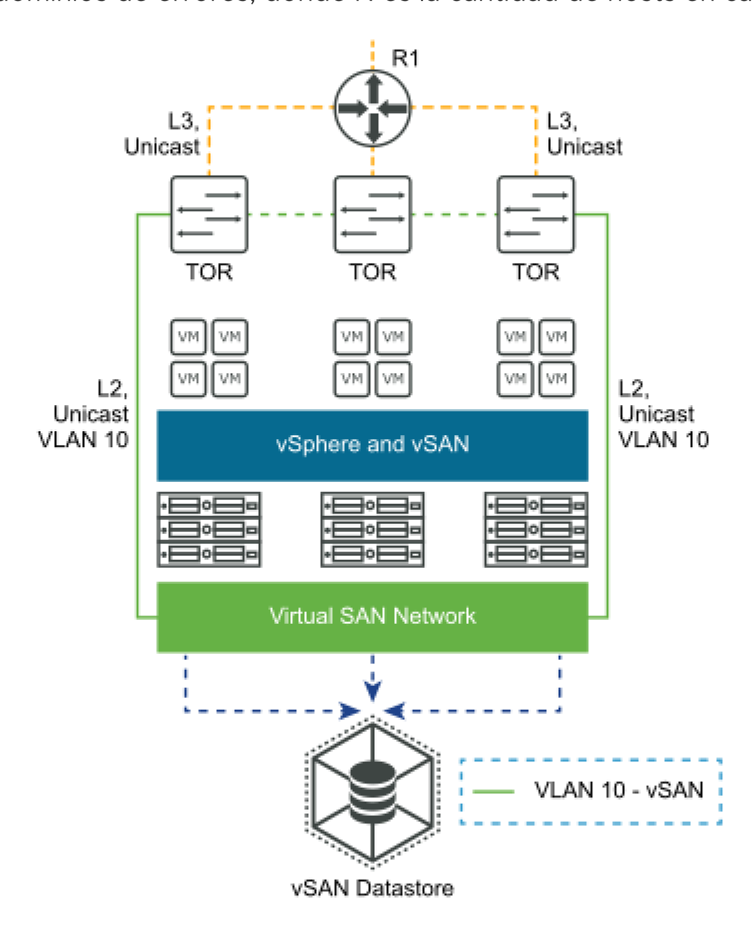
En el modo de unidifusión, el nodo principal se dirige a todos los nodos del clúster mientras envía el mismo mensaje a todos los nodos de vSAN en un clúster.

Por ejemplo, si N es el número de nodos de vSAN, el nodo principal enviará los mensajes N número de veces. Esto da como resultado un leve aumento del tráfico de CMMDS de vSAN. Es posible que no advierta este leve aumento del tráfico durante las operaciones normales con un estado estable.

## Tráfico dentro del clúster en un único bastidor

Si todos los nodos de un clúster de vSAN están conectados al mismo del conmutador de la parte superior de bastidor (TOR), el aumento total del tráfico solo se produce entre el nodo principal y el conmutador.

Si un clúster de vSAN abarca más de un conmutador TOR, se expandirá el tráfico entre el conmutador. Si un clúster abarca varios bastidores, varios TOR crean dominios de errores (FD) para el reconocimiento de los bastidores. El nodo principal envía N mensajes a los bastidores o dominios de errores, donde N es la cantidad de hosts en cada dominio de errores.

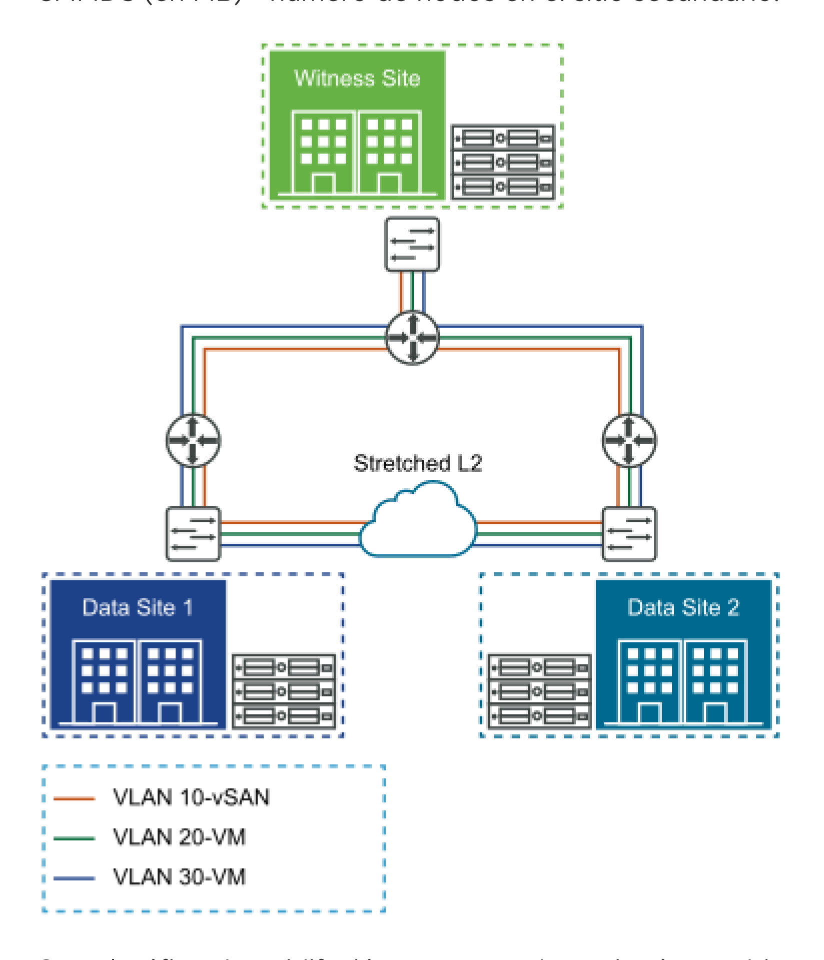



## Tráfico dentro de un clúster ampliado

En un clúster ampliado, el nodo principal se encuentra en el sitio de preferencia.

En un dominio de errores, los datos de CMMDS deben comunicarse del sitio secundario al sitio de preferencia. Para calcular el tráfico en un clúster ampliado, debe multiplicar el número de nodos de un sitio secundario por el tamaño del nodo de CMMDS (en MB) por el número de nodos en el sitio secundario.

Tráfico en un clúster ampliado = número de nodos en el sitio secundario * tamaño del nodo de CMMDS (en MB) * número de nodos en el sitio secundario.




Con el tráfico de unidifusión, no se produce ningún cambio en los requisitos de tráfico del sitio testigo.

# Configurar el transporte de red IP

6

Los protocolos de transporte proporcionan servicios de comunicación a través de la red. Estos servicios incluyen la pila de TCP/IP y el control de flujo.

Este capítulo incluye los siguientes temas:



## Pilas de TCP/IP de vSphere

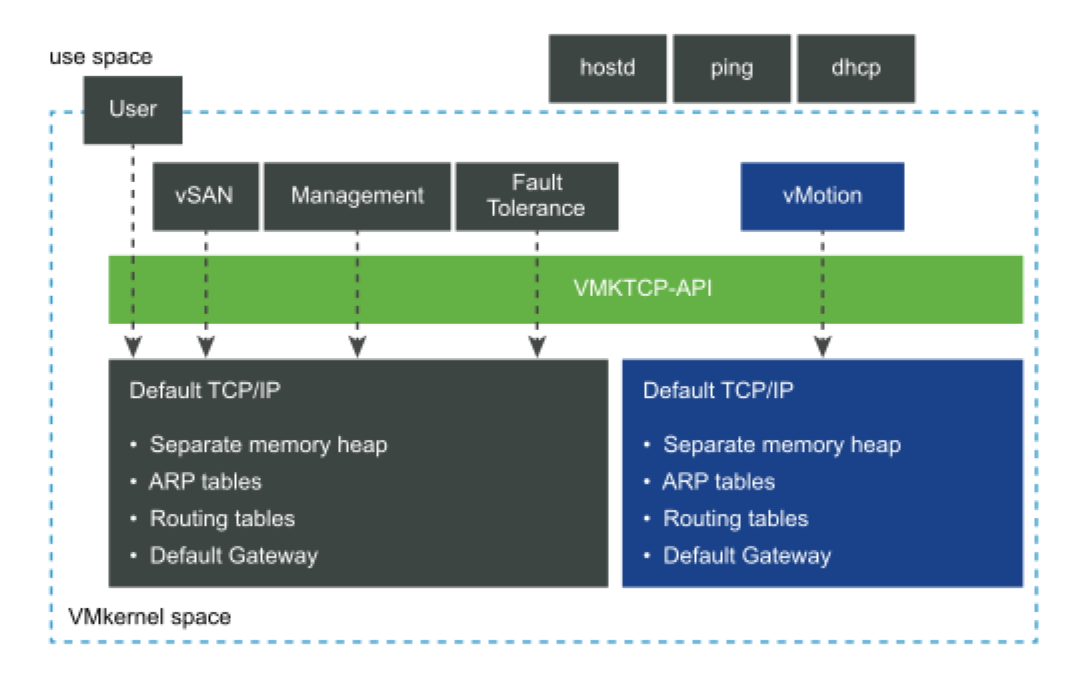
vSphere no incluye una pila de TCP/IP dedicada para el servicio de tráfico de vSAN. Puede agregar la interfaz de red de VMkernel de vSAN a la pila de TCP/IP predeterminada y definir rutas estáticas para todos los hosts del clúster de vSAN.

vSphere no admite la creación de una pila de TCP/IP personalizada vSAN. Puede garantizar que el tráfico de vSAN en las topologías de red de capa 3 deje de usar la interfaz de red de VMkernel de vSAN. Agregue la interfaz de red de VMkernel de vSAN a la pila de TCP/IP predeterminada y defina rutas estáticas para todos los hosts del clúster de vSAN.

**Nota** vSAN no tiene su propia pila de TCP/IP. Utilice rutas estáticas para enrutar el tráfico de vSAN en redes de capa 3.

vSphere 6.0 introdujo una nueva arquitectura de pila de TCP/IP que puede utilizar varias pilas de TPC/IP para administrar diferentes interfaces de red de VMkernel. Con esta arquitectura, puede configurar servicios de tráfico como vMotion, administración y tolerancia a errores en pilas de TCP/IP aisladas, que pueden usar varias puertas de enlace predeterminadas.

Para los requisitos de seguridad y aislamiento del tráfico de red, implemente los diferentes servicios de tráfico en diferentes segmentos de red o VLAN. Esto evitará que los diferentes servicios de tráfico atraviesen la misma puerta de enlace predeterminada.




Cuando configure los servicios de tráfico en diferentes pilas de TCP/IP, implemente cada tipo de servicio de tráfico en su propio segmento de red. A los segmentos de red se accede a través de un adaptador de red físico con segmentación de VLAN. Asigne cada segmento a diferentes interfaces de red de VMkernel con los respectivos servicios de tráfico habilitados.

## Pilas de TCP/IP disponibles en vSphere

vSphere proporciona pilas de TCP/IP que admiten requisitos de tráfico de vSAN.

- **Pila de TCP/IP predeterminada**. Administre los servicios de tráfico relacionados con el host. Esta pila comparte una sola puerta de enlace predeterminada entre todos los servicios de red configurados.
- **Pila de TCP/IP de vMotion**. Aísle el tráfico de vMotion en su propia pila. El uso de esta pila elimina o deshabilita completamente el tráfico de vMotion de la pila de TCP/IP predeterminada.
- **Pila de TCP/IP de aprovisionamiento**. Aísle algunas operaciones relacionadas con la máquina virtual, como las migraciones en frío, la clonación, la instantánea o el tráfico de NFC.

Puede seleccionar una pila de TCP/IP diferente durante la creación de una interfaz de VMkernel.

Los entornos con requisitos de red aislado para los servicios de tráfico de vSphere no pueden utilizar la misma puerta de enlace predeterminada para dirigir el tráfico. El uso de diferentes pilas de TCP/IP simplifica la administración del aislamiento del tráfico, ya que se pueden utilizar distintas puertas de enlace predeterminadas y evitar agregar rutas estáticas. Use esta técnica cuando tenga que enrutar el tráfico de vSAN a otra red a la que no se pueda acceder a través de la puerta de enlace predeterminada.

# vSphere RDMA

vSAN 7.0 Update 2 y versiones posteriores admiten la comunicación de acceso directo a memoria remota (RDMA).

RDMA permite el acceso directo a memoria desde la memoria de un equipo a la memoria de otro equipo sin involucrar al sistema operativo ni la CPU. La transferencia de memoria se descarga en los adaptadores de canal de host (HCA) compatibles con RDMA.

vSAN admite el protocolo RoCE v2. RoCE v2 requiere una red configurada para un funcionamiento sin pérdida.

Cada host de vSAN debe tener una NIC compatible con RDMA certificada por vSAN, tal como se indica en la sección de vSAN de la Guía de compatibilidad de VMware. Use solo los mismos adaptadores de red modelo del mismo proveedor en cada extremo de la conexión.

**Nota** vSphere RDMA no admite clústeres ampliados o de dos nodos de vSAN.

Todos los hosts del clúster deben admitir RDMA. Si algún host pierde la compatibilidad con RDMA, todo el clúster de vSAN cambiará a TCP.

vSAN con RDMA admite la conmutación por error de NIC, pero no la formación de equipos de NIC basada en hash de IP o LACP.

# Object Missing

This object is not available in the repository.

# Rutas estáticas

Puede utilizar rutas estáticas para permitir que las interfaces de red de vSAN de los hosts de una subred lleguen a los hosts de otra red.

La mayoría de las organizaciones separan la red de vSAN de la red de administración, por lo que la red de vSAN no tiene una puerta de enlace predeterminada. En una implementación de capa 3, los hosts que se encuentran en subredes o segmentos de capa 2 diferentes no pueden comunicarse entre sí a través de la puerta de enlace predeterminada, que normalmente está asociada a la red de administración.

Use *rutas estáticas* para permitir que las interfaces de red de vSAN de los hosts de una subred alcancen las redes de vSAN en los hosts de la otra red. Las rutas estáticas indican a un host cómo acceder a una red en particular a través de una interfaz en lugar de usar la puerta de enlace predeterminada.

En el siguiente ejemplo, se muestra cómo agregar una ruta estática de IPv4 a un host ESXi. Especifique la puerta de enlace (-g) y la red (-n) a la que desea acceder a través de la puerta de enlace :

```
esxcli network ip route ipv4 add –g 172.16.10.253 -n 192.168.10.0/24
```

Cuando se hayan agregado las rutas estáticas, la conectividad de tráfico de vSAN estará disponible en todas las redes, suponiendo que la infraestructura física lo permita. Ejecute el comando `vmkping` para probar y confirmar la comunicación entre las distintas redes. Para ello, haga ping a la dirección IP o la puerta de enlace predeterminada de la red remota. También puede comprobar paquetes de diferente tamaño (-s) y evitar la fragmentación (-d) del paquete.

```
vmkping –I vmk3 192.168.10.253
```

## Tramas gigantes

vSAN es totalmente compatible con tramas gigantes en la red de vSAN.

Las tramas gigantes son tramas Ethernet con más de 1500 bytes de carga útil. Las tramas gigantes normalmente transmiten hasta 9000 bytes de carga útil, pero existen variaciones.

El uso de tramas gigantes puede reducir el uso de la CPU y mejorar la capacidad de proceso.

Debe decidir si estos beneficios compensan la sobrecarga de implementar tramas gigantes en toda la red. En los centros de datos donde las tramas gigantes ya están habilitadas en la infraestructura de red, puede utilizarlas para vSAN. El coste operativo de configurar tramas gigantes en toda la red puede compensar los limitados beneficios de CPU y rendimiento.

# Object Missing

7

This object is not available in the repository.

# Usar el control de congestión y el control de flujo

8

Utilice el control de flujo para administrar la velocidad de la transferencia de datos entre los remitentes y los receptores de la red de vSAN. El control de congestión controla la congestión en la red.

## Control del flujo

Puede usar el control de flujo para administrar la velocidad de transferencia de datos entre dos dispositivos.

El control de flujo se configura cuando dos dispositivos conectados físicamente ejecutan la negociación automática.

Un nodo de red sobrecargado puede enviar una trama de pausa para detener la transmisión del remitente durante un periodo determinado. Una trama con una dirección de destino de multidifusión enviada a un conmutador se reenvía a través de los demás puertos del conmutador. Las tramas de pausa tienen una dirección de destino de multidifusión especial que las distingue de otros tráfico de multidifusión. Un conmutador que cumpla las directivas no reenvía una trama de pausa. Las tramas enviadas a este rango solo se deben tratar dentro del conmutador. Las tramas de pausa tienen una duración limitada y caducan después de un intervalo de tiempo. Dos equipos conectados a través de un conmutador nunca envían tramas de pausa entre sí, pero pueden enviarlas a un conmutador.

Una razón para utilizar las tramas de pausa es la compatibilidad con controladoras de interfaz de red (NIC) que no tienen suficiente memoria intermedia para controlar la recepción a toda velocidad. Este problema no es habitual con las mejoras en las velocidades de bus y los tamaños de memoria.

## Control de congestión

El control de congestión permite controlar el tráfico en la red.

El control de congestión se aplica principalmente a redes de conmutación de paquetes. La congestión de la red en un conmutador podría deberse a los vínculos entre conmutadores sobrecargados. Si los vínculos entre conmutadores sobrecargan la capacidad en la capa física, el conmutador introducirá tramas de pausa para protegerse.

## Control de flujo basado en prioridad

El control de flujo basado en prioridad (PFC) ayuda a eliminar la pérdida de tramas debido a la congestión.

El control de flujo basado en prioridades (IEEE 802.1Qbb) se logra mediante un mecanismo similar a las tramas de pausa, pero funciona en prioridades individuales. El PFC también se denomina control de flujo basado en clases (CBFC) o por pausa de prioridad (PPP).

## Control de flujo y control de congestión

El control de flujo es un mecanismo de extremo a extremo que controla el tráfico entre un remitente y un destinatario. El control de flujo se produce en la capa de vínculo de datos y en la capa de transporte.

El control de congestión se utiliza para controlar la congestión en una red. Este problema no es tan común en redes modernas con mejoras en velocidades de bus y tamaños de memoria. Un escenario más probable es la congestión de la red dentro de un conmutador. El control de congestión se gestiona mediante la capa de red y la capa de transporte.

## Consideraciones de diseño de control de flujo

De forma predeterminada, el control de flujo está habilitado en todas las interfaces de red de los hosts ESXi.

La configuración del control de flujo en una NIC se realiza mediante el controlador. Cuando una NIC se satura por el tráfico de red, la NIC envía tramas de pausa.

Los mecanismos de control de flujo, como las tramas de pausa, pueden activar la latencia general en la E/S de invitado de la máquina virtual debido a la mayor latencia en la capa de red de vSAN. Algunos controladores de red proporcionan opciones de módulo que configuran la funcionalidad del control de flujo dentro del controlador. Algunos controladores de red permiten modificar las opciones de configuración mediante la utilidad de la línea de comandos `ethtool` en la consola del host ESXi. Utilice las opciones del módulo o `ethtool`, en función de los detalles de implementación de cada controlador.

Para obtener información sobre la configuración de control de flujo en hosts ESXi, consulte el artículo 1013413 de la base de conocimientos de VMware.

En implementaciones con 1 Gbps, deje el control de flujo habilitado en las interfaces de red de ESXi (valor predeterminado). Si las tramas de pausa son un problema, planee cuidadosamente la deshabilitación del control de flujo junto con el servicio de soporte del proveedor de hardware o con el servicio de soporte global de VMware.

Para saber cómo reconocer si se están enviando tramas de pausa de un receptor a un host ESXi, consulte Capítulo 13 Solución de errores de las redes vSAN. Un gran número de tramas de pausa en un entorno indica normalmente una red o un problema de transporte subyacente que hay que investigar.

# Formación de equipos de NIC básica, conmutación por error y equilibrio de carga

9

Muchos entornos vSAN requieren de algún nivel de redundancia de red.

Puede utilizar la formación de equipos de NIC para lograr la redundancia de red. Puede configurar dos o más adaptadores de red (NIC) como un equipo para obtener un alto nivel de disponibilidad y equilibrio de carga. La formación de equipos de NIC básica está disponible con redes de vSphere, y estas técnicas pueden afectar al diseño y la arquitectura de vSAN.

Hay disponibles varias opciones de formación de equipos de NIC. Evite las directivas de formación de equipos de NIC que requieran configuraciones de conmutador físico o que necesiten comprender los conceptos de redes, como la adición de enlaces. Los mejores resultados se obtienen con una configuración básica, simple y fiable.

Si no está seguro de las opciones de formación de equipos de NIC, utilice una configuración Activo/En espera con conmutación por error explícita.

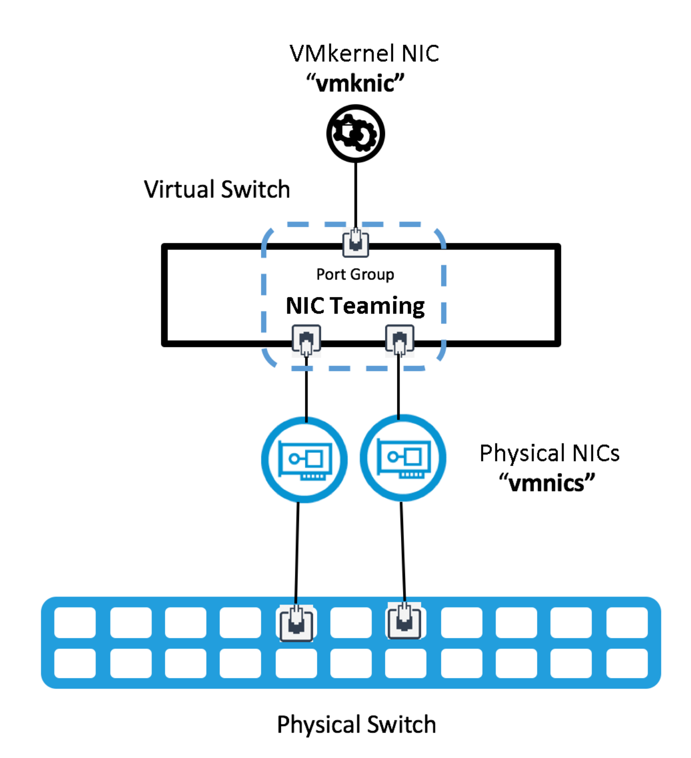
Este capítulo incluye los siguientes temas:



## Formación de equipos de NIC básica

La formación de equipos de NIC básica utiliza varios vínculos superiores físicos, un vmknic y un solo conmutador.

La formación de equipos de NIC de vSphere utiliza varios adaptadores de vínculo superior, llamados vmnics, que se asocian con un solo conmutador virtual para formar un equipo. Esta es la opción más básica y puede configurarla con un conmutador estándar de vSphere o un conmutador distribuido de vSphere (vDS).




## Conmutación por error y redundancia

vSAN puede utilizar la directiva básica de formación de equipos y conmutación por error de NIC que ofrece vSphere.

La formación de equipos de NIC en un vSwitch puede tener varios vínculos superiores activos o una configuración de vínculo superior Activo/En espera. La formación de equipos de NIC básica no requiere ninguna configuración especial en la capa del conmutador físico.

**Nota** vSAN no utiliza la formación de equipos de NIC para el equilibrio de carga.

Una configuración de formación de equipos de NIC típica dispone de las siguientes opciones. Cuando trabaje en conmutadores distribuidos, edite la configuración del grupo de puertos distribuidos que se utiliza para el tráfico de vSAN.

- Equilibrio de carga: Enrutar según el puerto virtual de origen
- Detección de errores de red: Solo estado de vínculo
- Notificar a conmutadores: Sí
- Conmutación por recuperación: Sí

Tráfico de vSAN de equilibrio de carga

- Equilibrio de carga: Enrutar según el puerto virtual de origen
- Detección de errores de red: Solo estado de vínculo
- Notificar a conmutadores: Sí
- Conmutación por recuperación: Sí

# Configurar el equilibrio de carga para equipos de NIC

Hay varias técnicas de equilibrio de carga disponibles para la formación de equipos de NIC, y cada una tiene sus ventajas e inconvenientes.

## Enrutar según el puerto virtual de origen

En configuraciones activas/activas o activas/pasivas, utilice **Enrutar según el puerto virtual de origen** para la formación de equipos de NIC básica. Cuando esta directiva está vigente, solo se utilizará una NIC física por cada puerto de VMkernel.

**Ventajas**

- Este es el método de formación de equipos de NIC más simple que requiere una configuración mínima del conmutador físico.
- Este método solo requiere un puerto único para el tráfico de vSAN, lo que simplifica la solución de problemas.

**Inconvenientes**

- Una única interfaz de VMkernel está limitada al ancho de banda de una sola NIC física. Como los entornos de vSAN típicos utilizan un adaptador de VMkernel, solo se utiliza una NIC física en el equipo.

## Enrutar según la carga de la NIC física

**Enrutar según la carga de la NIC física** se basa en **Enrutar según el puerto virtual de origen**, en el que el conmutador virtual supervisa la carga real de los vínculos superiores y sigue los pasos para reducirla en los vínculos superiores sobrecargados. Este método de equilibrio de carga solo está disponible con vSphere Distributed Switch, no con los conmutadores estándar de vSphere.

El conmutador distribuido calcula los vínculos superiores de cada puerto de VMkernel usando el identificador de puerto y el número de vínculos superiores en el equipo de la NIC. El conmutador distribuido comprueba los vínculos superiores cada 30 segundos. Si la carga supera el 75 %, el identificador de VMkernel con la E/S más alta se transfiere a otro vínculo superior.

**Ventajas**

- No se requiere ninguna configuración de conmutador físico.
- Aunque vSAN tiene un puerto de VMkernel, otros puertos de VMkernel o servicios de red pueden compartir los mismos vínculos superiores. vSAN puede beneficiarse del uso de otros vínculos superiores de otros servicios, como vMotion o administración.

**Inconvenientes**

- Dado que vSAN por lo general solo tiene configurado un puerto de VMkernel, su eficacia es limitada.
- El VMkernel de ESXi vuelve a evaluar la carga de tráfico después de cada intervalo de tiempo, lo que puede causar una sobrecarga de procesamiento.

## Configuración: Detección de errores de red

Utilice la configuración predeterminada: **Solo estado de vínculo**. No utilice sondeo de señal para la detección de errores de vínculos. El sondeo de señal requiere al menos tres NIC físicas para evitar escenarios de cerebro dividido. Para obtener más información, consulte el artículo 1005577 de la base de conocimientos de VMware.

## Configuración: Notificar a conmutadores

Utilice la configuración predeterminada: **Sí**. Los conmutadores físicos tienen tablas de reenvío de direcciones MAC para asociar cada dirección MAC a un puerto de conmutador físico. Cuando se recibe una trama, el conmutador determina la dirección MAC de destino en la tabla y decide el puerto físico correcto.

Si se produce una conmutación por error de NIC, el host ESXi debe notificar a los conmutadores de red que algo ha cambiado, o el conmutador físico puede seguir usando la información antigua y enviar las tramas al puerto incorrecto.

Cuando se establece Notificar a conmutadores en **Sí**, si una NIC física falla y el tráfico se vuelve a enrutar a otra NIC física del equipo, el conmutador virtual envía notificaciones por medio de la red para actualizar las tablas de búsqueda en los conmutadores físicos.

Esta opción no captura las configuraciones erróneas de VLAN ni las pérdidas de vínculos superiores que se producen en el flujo ascendente adicional en la red. La comprobación de estado de las particiones de red de vSAN puede detectar estos problemas.

## Configuración: Conmutación por recuperación

Esta opción determina de qué forma un adaptador físico vuelve a activarse después de recuperarse de un error. Un evento de conmutación por error activa el tráfico de red para pasar de una NIC a otra. Cuando se detecta un estado **Vínculo activo** en la NIC de origen, el tráfico se revierte automáticamente al adaptador de red original cuando la conmutación por recuperación se establece en **Sí**. Si la conmutación por recuperación se establece en **No**, es necesario realizar una conmutación por error manual.

Configurar la conmutación por recuperación en **No** puede ser útil en algunas situaciones. Por ejemplo, después de que un puerto del conmutador físico se recupere de un error, el puerto puede estar activo, pero puede tardar varios segundos en reenviar el tráfico. Se ha comprobado que la conmutación por recuperación automática causa problemas en ciertos entornos que utilizan el protocolo de árbol de expansión. Para obtener más información sobre el protocolo de árbol de expansión (STP), consulte el artículo 1003804 de la base de conocimientos de VMware.

## Configurar el orden de conmutación por error

El orden de conmutación por error determina qué vínculos estarán activos durante las operaciones normales y cuáles estarán activos en caso de una conmutación por error. Se pueden utilizar diferentes configuraciones admitidas para la red de vSAN.

**Vínculos superiores activos/en espera**: Si se produce un error en una configuración activa/en espera, el controlador de NIC notifica a vSphere de un evento de vínculo inactivo en el vínculo superior 1. El vínculo superior en espera 2 se activa y el tráfico se reanuda en el vínculo superior 2.

**Vínculos superiores activos/activos**: Si establece el orden de conmutación por error en Activo/Activo, el puerto virtual utilizado por el tráfico de vSAN no puede utilizar ambos puertos físicos al mismo tiempo.

Si la configuración de formación de equipos de NIC para el vínculo superior 1 y el vínculo superior 2 está activa, no es necesario que el vínculo superior en espera se active.

---

**Nota** Cuando se utiliza una configuración Activo/Activo, asegúrese de que la conmutación por recuperación se establece en **No**. Para obtener más información, consulte el artículo 2072928 de la base de conocimientos de VMware.

---

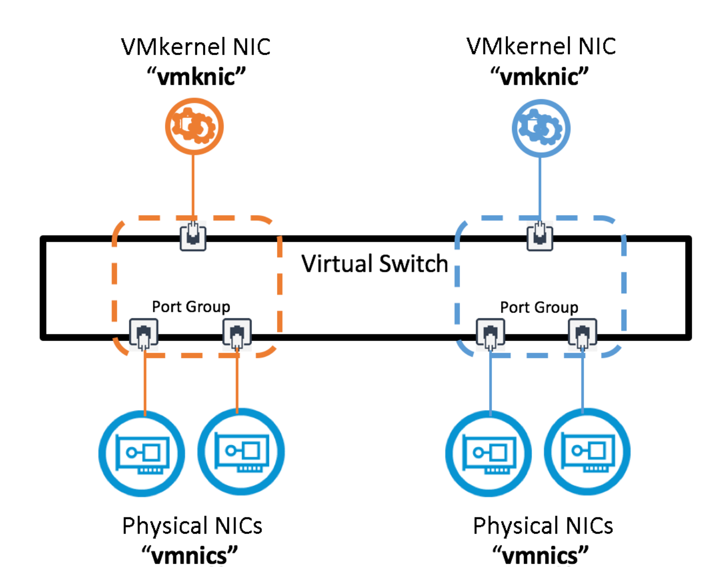
# Formación de equipos de NIC avanzada

10

Puede utilizar métodos avanzados de formación de equipos de NIC con varios adaptadores de VMkernel para configurar la red de vSAN. Si utiliza el protocolo de adición de enlaces (LAG/ LACP), la red vSAN puede configurarse con un solo adaptador de VMkernel.

Puede utilizar la formación de equipos de NIC avanzada para implementar un aislamiento, de modo que un error que se produzca en una ruta de red no afecte a la otra ruta. Si se produce un error en alguna parte de una ruta de red, la otra ruta podrá transportar el tráfico. Configure varias NIC de VMkernel para vSAN en diferentes subredes, como otra VLAN o un tejido de red física independiente.

vSphere y vSAN no admiten varios adaptadores de VMkernel (vmknics) en la misma subred. Para obtener más información, consulte el artículo de la base de conocimientos de VMware 2010877.




Este capítulo incluye los siguientes temas:

- Información sobre el grupo de adición de enlaces
- Información sobre los aislamientos de red
- Ventajas e inconvenientes de las configuraciones de red aislada vSAN

- Ejemplos de configuración de formación de equipos de NIC

# Información sobre el grupo de adición de enlaces

Al usar el protocolo LACP, un dispositivo de red puede negociar una agrupación automática de vínculos mediante el envío de paquetes LACP a un elemento del mismo nivel.

Un grupo de adición de enlaces (LAG) se define mediante el estándar IEEE 802.1AX-2008, que establece que la adición de enlaces permite que uno o varios vínculos se agreguen juntos para crear un grupo de adición de enlaces.

El LAG se puede configurar como estático (manual) o dinámico usando LACP para negociar la formación de LAG. LACP puede configurarse de la siguiente forma:

**Activo**

Los dispositivos envían mensajes LACP inmediatamente cuando se activa el puerto. Los dispositivos finales con LACP habilitado (por ejemplo, hosts ESXi y conmutadores físicos) envían y reciben entre sí tramas denominadas mensajes LACP para negociar la creación de un LAG.

**Pasivo**

Los dispositivos colocan un puerto en un estado de negociación pasiva, en el que el puerto solo responde a los mensajes LACP recibidos, pero no inicia la negociación.

**Nota** Si el host y el conmutador están en modo pasivo, el LAG no se inicializa, ya que se requiere una parte activa para iniciar la vinculación. Al menos uno debe ser activo.

En vSphere 5.5 y versiones posteriores, esta función se denomina **LACP mejorado**. Esta función solo se admite vSphere Distributed Switch 5.5 o versiones posteriores.

Para obtener más información sobre la compatibilidad con LACP en un vSphere Distributed Switch, consulte la documentación sobre redes de vSphere 6.

**Nota** El número de LAG que se pueden utilizar depende de la capacidad del entorno físico subyacente y de la topología de la red virtual.

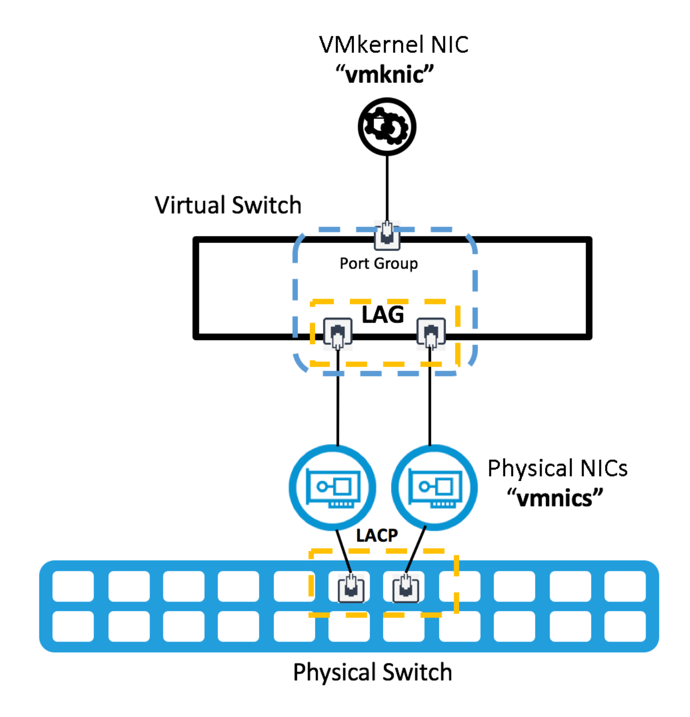
Para obtener más información sobre las diferentes opciones de equilibrio de carga, consulte el artículo 2051826 de la base de conocimientos.

## Adición de enlaces estáticos y dinámicos

Puede utilizar LACP para combinar y agregar varias conexiones de red.

Cuando LACP está en modo **activo** o **dinámico**, un conmutador físico envía mensajes LACP a los dispositivos de red, como los hosts ESXi, para negociar la creación de un grupo de adición de enlaces (LAG).

Para configurar la adición de enlaces en hosts mediante conmutadores estándar de vSphere (y conmutadores anteriores a vSphere Distributed Switch 5.5), configure un grupo de canales estático en el conmutador físico. Para obtener más información, consulte la documentación del proveedor.




## Ventajas y desventajas de la adición de enlaces dinámicos

Tenga en cuenta los siguientes inconvenientes de usar la adición de enlaces dinámicos.

### Ventajas

**Mejora el rendimiento y el ancho de banda**. Un puerto de VMkernel o host vSAN puede comunicarse con muchos otros hosts vSAN usando gran variedad de opciones de equilibrio de carga diferentes.

**Proporciona redundancia de adaptador de red**. Si se produce un error en una NIC y el estado del vínculo es erróneo, el resto de las NIC del equipo continuarán transmitiendo tráfico.

**Mejora el equilibrio del tráfico**. El equilibrio del tráfico después de que se produzcan errores es rápido y automático.

### Inconvenientes

**Es menos flexible**. La configuración del conmutador físico requiere que este estén configurados en una configuración de canal de puerto.

**Es más complejo**. El uso de varios conmutadores para producir una configuración de redundancia física completa es complejo. Las implementaciones específicas del proveedor agregan más complejidad.

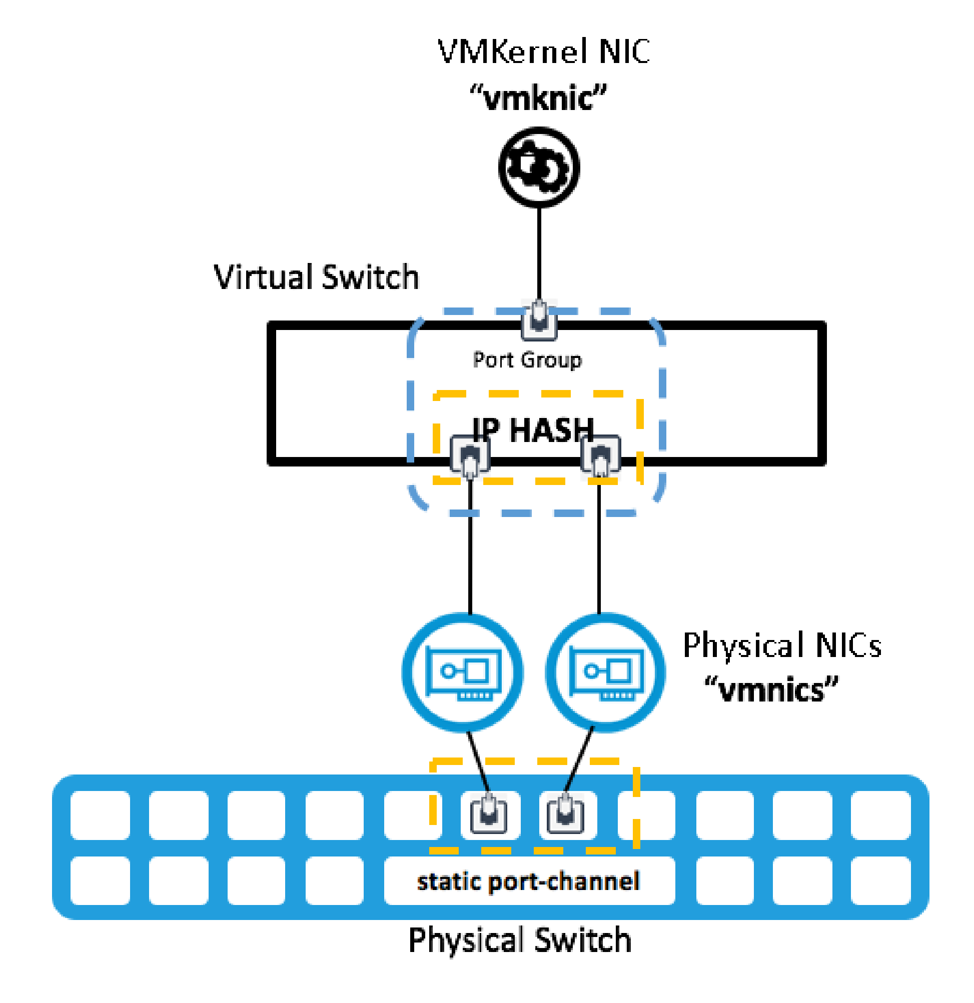
# LACP estático con Enrutar según el hash de IP

Puede crear un clúster de vSAN 6.6 mediante LACP estático con una directiva de hash de IP. Esta sección se centra en conmutadores estándar de vSphere, pero también puede utilizar los conmutadores distribuidos de vSphere.

Puede utilizar la directiva de equilibrio de carga Enrutar según el hash de IP. Para obtener más información sobre el hash de IP, consulte la documentación de vSphere .

Seleccione la directiva de equilibrio de carga **Enrutar según el hash de IP** en un nivel de grupo de puertos o vSwitch. Establezca todos los vínculos superiores asignados al grupo de canales estáticos en la posición Vínculo superior activo en las directivas de formación de equipos y conmutación por error en el nivel del grupo de puertos o del conmutador virtual.

Cuando se configura el hash de IP en un grupo de puertos de vSphere, el grupo de puertos utilizará la directiva **Enrutar según el hash de IP**. La cantidad de puertos del canal de puertos debe ser igual a la cantidad de vínculos superiores del equipo.




## Ventajas e inconvenientes de LACP estático con hash de IP

Tenga en cuenta los inconvenientes de usar LACP estático con el hash de IP.

### Ventajas

- **Mejora el rendimiento y el ancho de banda**. Un puerto de VMkernel o host vSAN puede comunicarse con muchos otros hosts vSAN usando el algoritmo de hash de IP.
- **Proporciona redundancia de adaptador de red**. Si se produce un error en una NIC y el estado del vínculo es erróneo, el resto de las NIC del equipo continuarán transmitiendo tráfico.
- **Agrega flexibilidad**. Puede usar hash de IP con los conmutadores estándar de vSphere y con vSphere Distributed Switch.

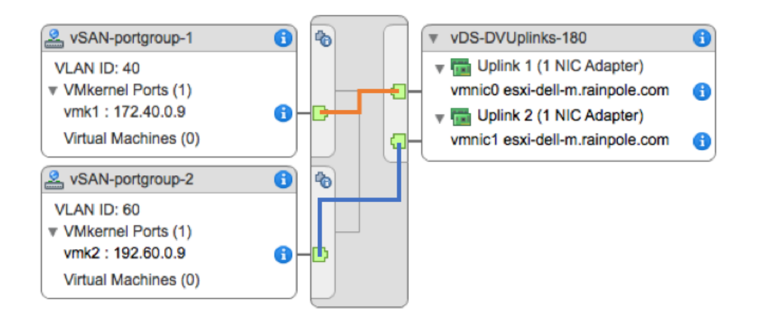
### Inconvenientes

- **La configuración del conmutador físico es menos flexible**. Los puertos del conmutador físico deben configurarse en una configuración de canal de puerto estático.
- **Mayor probabilidad de configuraciones erróneas**. Los canales de puerto estático se crean sin ninguna verificación en ninguno de los extremos (a diferencia del canal de puerto dinámico de LACP).
- **Es más complejo**. Introducir la configuración de redundancia física completa aumenta la complejidad cuando se utilizan varios conmutadores. Las implementaciones pueden ser específicas del proveedor.
- **Equilibrio de carga limitado**. Si el entorno tiene pocas direcciones IP, es posible que el conmutador virtual haga pasar constantemente el tráfico por un mismo vínculo superior del equipo. Esto puede darse especialmente en clústeres de vSAN pequeños.

## Información sobre los aislamientos de red

Puede usar métodos avanzados de formación de equipos de NIC para crear un tejido de almacenamiento con aislamiento. Se utilizan dos redes de almacenamiento para crear una topología de red de almacenamiento redundante, donde cada una se aísla tanto física como lógicamente de la otra mediante un aislamiento.

Puede configurar un aislamiento de red para vSAN en un entorno de vSphere. Configure varios puertos de VMkernel de por cada host de vSAN. Asocie cada puerto de VMkernel a vínculos superiores físicos dedicados mediante una sola instancia de vSwitch o varios conmutadores virtuales, tanto conmutadores estándar de vSphere como vSphere Distributed Switch .



Por lo general, cada vínculo superior debe estar conectado a una infraestructura física totalmente redundante.

Esta topología no es la idónea. El error de componentes como las NIC en diferentes hosts que residen en la misma red puede producir la interrupción de E/S de almacenamiento. Para evitar este problema, implemente redundancia de las NIC físicas en todos los hosts y todos los segmentos de red. El ejemplo de configuración 2 aborda esta topología en detalle.

Estas configuraciones se aplican a las topologías de capa 2 y capa 3, con configuraciones de unidifusión y multidifusión.

# Ventajas e inconvenientes de las configuraciones de red aislada vSAN

Los aislamientos de red pueden resultar útiles para separar y aislar el tráfico de vSAN. Tenga cuidado al configurar esta topología.

**Ventajas**

- Separación física y lógica del tráfico de vSAN.

**Inconvenientes**

- vSAN no admite varios adaptadores de VMkernel (vmknics) en la misma subred. Para obtener más información, consulte el artículo 2010877 de la base de conocimientos de VMware.
- Esta configuración es compleja y propensa a errores, por lo que la solución de problemas resulta más difícil.
- No se garantiza la disponibilidad de la red con varios vmknics en algunos errores asimétricos, como un error de NIC en un host y otro error de NIC en otro host.
- No se garantiza el tráfico de vSAN con equilibrio de carga en las NIC físicas.
- Los costes aumentan en los hosts de vSAN, ya que es posible que se necesiten varios adaptadores de VMkernel (vmknics) para proteger varias NIC físicas (vmnics). Por ejemplo, es posible que se necesiten 2x2 vmnics para proporcionar redundancia para dos vmknics de vSAN.
- Los recursos lógicos requeridos se duplican, como los puertos de VMkernel, las direcciones IP y las VLAN.
- vSAN no implementa la vinculación de puertos. Esto significa que técnicas como las rutas múltiples no están disponibles.
- Las topologías de capa 3 no son adecuadas para el tráfico de vSAN con varios vmknics. Es posible que estas topologías no funcionen según lo esperado.
- Es posible que se requiera la configuración del host de la línea de comandos para cambiar las direcciones de multidifusión de vSAN.

El LACP dinámico combina o agrega varias conexiones de red en paralelo para aumentar la capacidad de proceso y proporcionar redundancia. Cuando la formación de equipos de NIC está configurada con LACP, se produce un equilibrio de carga de la red de vSAN en varios vínculos superiores. Este equilibrio de carga se produce en la capa de red y no se realiza a través de vSAN.

**Nota** Otros términos que a veces se usan para describir la adición de enlaces son troncalización de puertos, unión de vínculos, enlace Ethernet/red/NIC o EtherChannel.

Esta sección se centra en el protocolo de control de adición de enlaces (LACP). El estándar IEEE es 802.3ad, pero algunos proveedores tienen funciones de LACP patentadas, como PAgP (protocolo de adición de puertos). Siga las prácticas recomendadas por el proveedor.

**Nota** La compatibilidad con LACP introducida en vSphere Distributed Switch 5.1 solo admite el equilibrio de carga de hash de IP. vSphere Distributed Switch 5.5 y versiones posteriores admiten LACP por completo.

LACP es un estándar de la industria que utiliza canales de puertos. Hay muchos algoritmos de hash disponibles. La directiva de grupo y puerto de vSwitch y la configuración del canal de puerto deben concordar y coincidir.

# Ejemplos de configuración de formación de equipos de NIC

Las siguientes configuraciones de formación de equipos de NIC ilustran escenarios típicos de redes de vSAN.

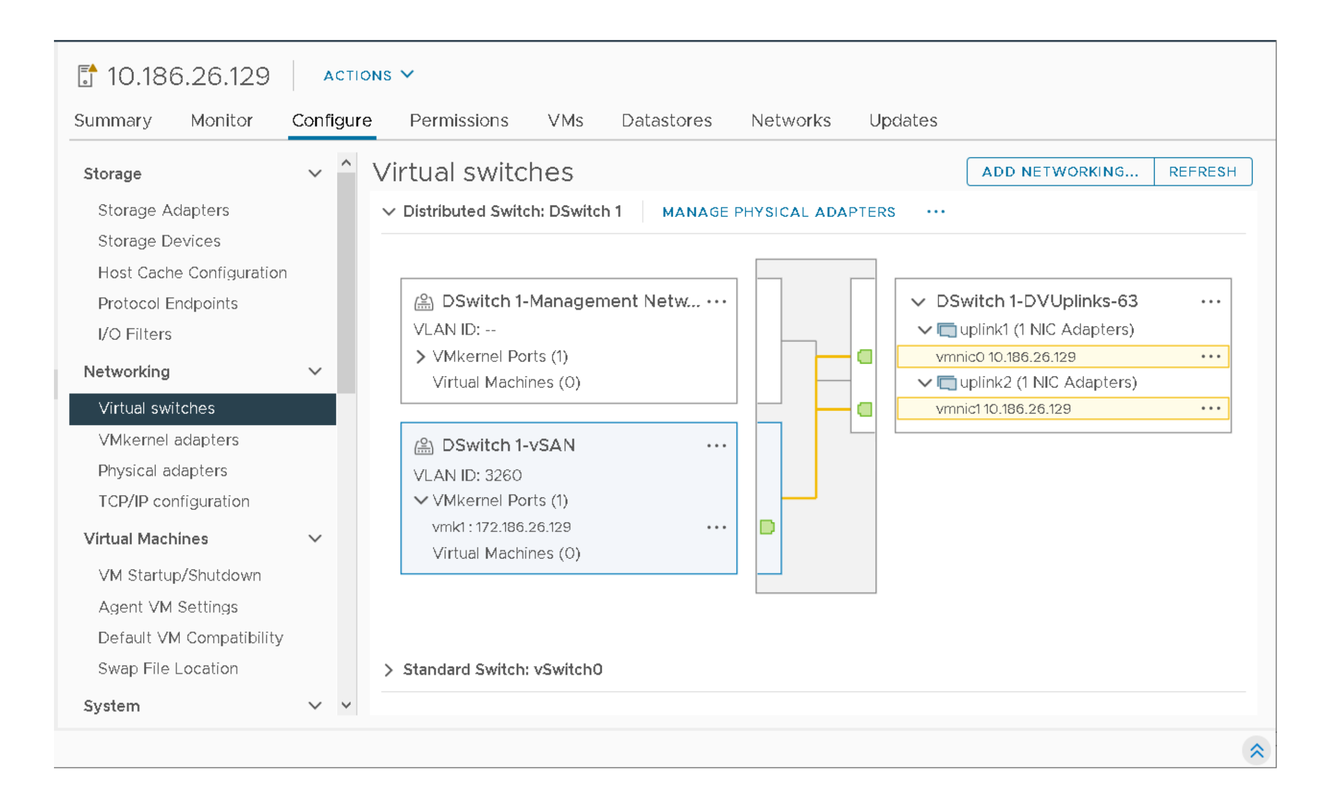
## Configuración 1: vmknic única, Enrutar según la carga de la NIC física

Puede configurar la formación de equipos de NIC activos/activos básicos con la directiva **Enrutar según la carga de la NIC física** para hosts vSAN. Utilice un vSphere Distributed Switch (vDS).

Para este ejemplo, el vDS debe tener dos vínculos superiores configurados para cada host. Un grupo de puertos distribuidos se designa para tráfico de vSAN y se aísla en una VLAN específica. Las tramas gigantes ya están habilitadas en el vDS con un valor de MTU de 9000.

Configure la formación de equipos y la conmutación por error del grupo de puertos distribuidos para el tráfico de vSAN siguiendo estos pasos:

- Directiva de equilibrio de carga: **Enrutar según la carga de la NIC física**.
- Detección de errores de red: **Solo estado de vínculo**.
- Notificar a conmutadores: **Sí**.
- Conmutación por recuperación: **No**. Puede establecer la conmutación por recuperación en **Sí**, pero no para este ejemplo.
- Asegúrese de que los dos vínculos superiores se encuentren en la posición **Vínculos superiores activos**.




## Pérdida de redundancia de vínculo superior de red

Cuando se detecta el estado de vínculo inactivo, la carga de trabajo cambia de un vínculo superior a otro. No hay ningún impacto apreciable en el clúster de vSAN ni en la carga de trabajo de la máquina virtual.

## Recuperación y conmutación por recuperación

Si establece **Conmutación por recuperación** en **No**, el tráfico no volverá a la vmnic original. Si se establece **Conmutación por recuperación** en **Sí**, el tráfico volverá a la vmnic original en la recuperación.

## Equilibrio de carga

Dado que se trata de una única NIC de VMkernel, no se obtienen beneficios de rendimiento al usar **Enrutar según la carga de la NIC física**.

Solo hay una NIC física en uso a la vez. La otra NIC física está inactiva.

# Configuración 2: varios vmknics, Enrutar según el identificador de puerto de origen

Puede utilizar dos VLAN no enrutables que están separadas de forma lógica y de forma física para generar una topología de aislamiento.

En este ejemplo se indican los pasos de configuración para un vSphere Distributed Switch, pero también se pueden utilizar conmutadores estándar de vSphere. Utiliza dos NIC físicas de 10 GB y las separa de forma lógica en la capa de redes de vSphere.

Cree dos grupos de puertos distribuidos para cada vmknic de VMkernel de vSAN. Cada grupo de puertos tiene una etiqueta de VLAN independiente. Para la configuración de VMkernel de vSAN, se requieren dos direcciones IP en ambas VLAN para el tráfico de vSAN.

**Nota** Las implementaciones prácticas suelen utilizar cuatro vínculos superiores físicos para obtener una redundancia completa.

Para cada grupo de puertos, la directiva de formación de equipos y conmutación por error utiliza la configuración predeterminada.

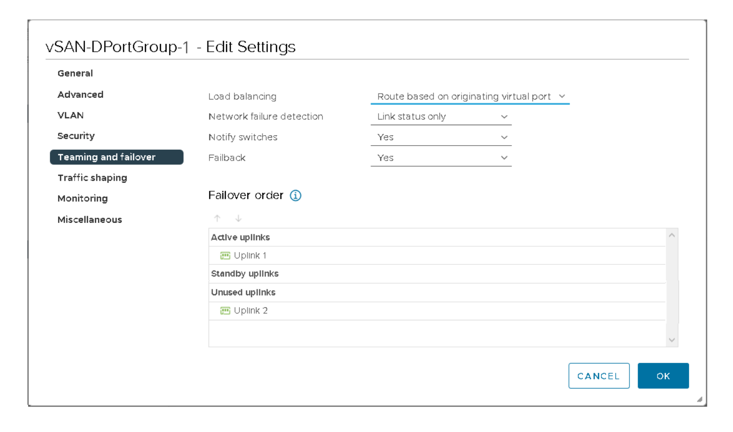
- Equilibrio de carga: **Enrutar según el identificador de puerto de origen**
- Detección de errores de red: **Solo estado de vínculo**
- Notificar a conmutadores: **Sí** (valor predeterminado)
- Conmutación por recuperación: **Sí** (valor predeterminado)
- La configuración del vínculo superior tiene un vínculo superior en la posición **Activo** y otro en la posición **Sin utilizar**.

Una red está totalmente aislada de la otra red.

## Grupo de puertos 1 de vSAN

En este ejemplo, se utiliza un grupo de puertos distribuidos llamado **vSAN-DPortGroup-1**. **VLAN 3266** está etiquetado para este grupo de puertos con la siguiente directiva de formación de equipos y conmutación por error:

- Tráfico en el grupo de puertos etiquetado con VLAN 3266
- Equilibrio de carga: **Enrutar según el identificador de puerto de origen**
- Detección de errores de red: **Solo estado de vínculo**
- Notificar a conmutadores: **Sí** (valor predeterminado)
- Conmutación por recuperación: **Sí** (valor predeterminado)
- La configuración del vínculo superior tiene el **vínculo superior 1** en la posición **Activo** y el **vínculo superior 2** en la posición **Sin utilizar**.



## Grupo de puertos 2 de vSAN

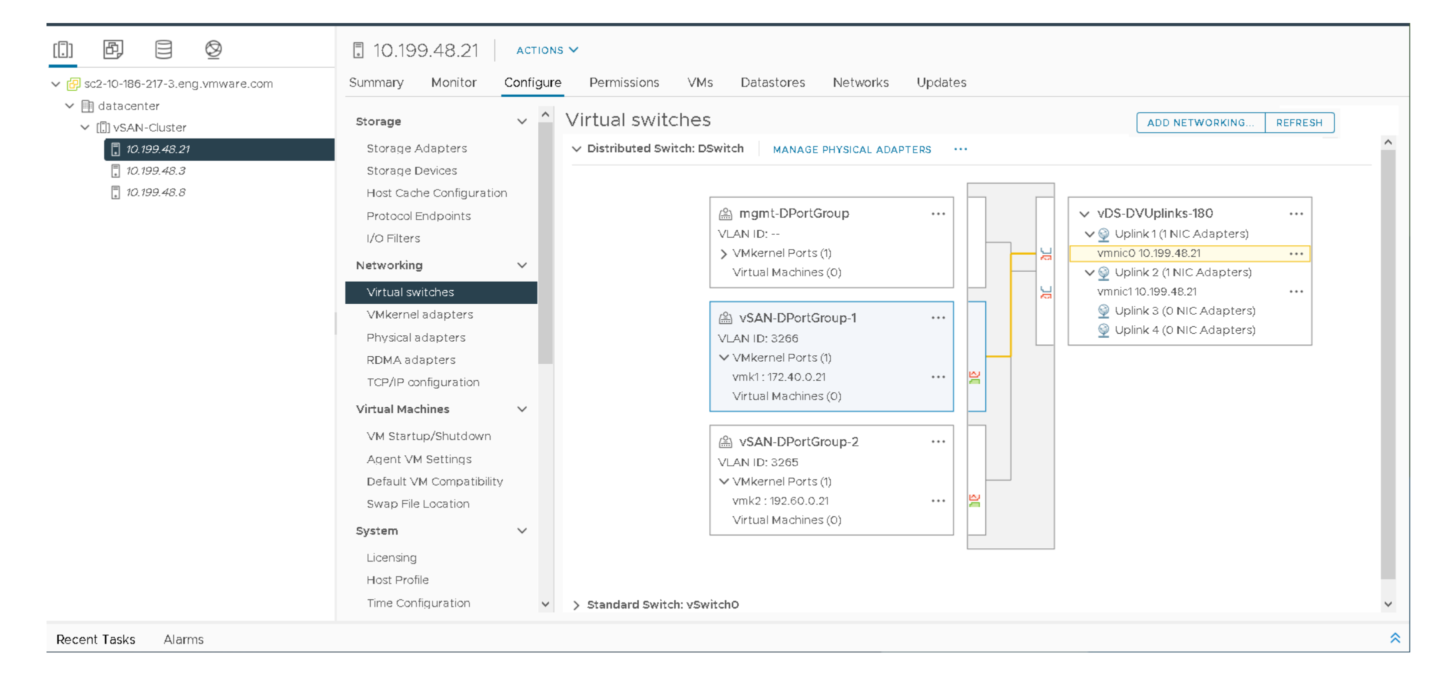
Para complementar el grupo de puertos 1 de vSAN, configure un segundo grupo de puertos distribuidos llamado **vSAN-portgroup-2** con las siguientes diferencias:

- Tráfico en el grupo de puertos etiquetado con VLAN 3265
- La configuración del vínculo superior tiene el **vínculo superior 2** en la posición **Activo** y el **vínculo superior 1** en la posición **Sin utilizar**.

## Configuración de puerto de VMkernel de vSAN

Cree dos interfaces de vSAN VMkernel en ambos grupos de puertos. En este ejemplo, los grupos de puertos se llaman **vmk1** y **vmk2**.

- **vmk1** está asociado a VLAN 3266 (172.40.0.xx) y, como resultado, al grupo de puertos **vSAN-DPortGroup-1**.
- **vmk2** está asociado a VLAN 3265 (192.60.0.xx) y, como resultado, al grupo de puertos **vSAN-DPortGroup-2**.




## Equilibrio de carga

vSAN no tiene ningún mecanismo de equilibrio de carga para diferenciar entre varios vmknics, por lo que la ruta de E/S de vSAN seleccionada no es determinista en las NIC físicas. Los gráficos de rendimiento de vSphere muestran que una NIC física suele utilizarse más que la otra. Una sencilla prueba de E/S realizada en nuestros laboratorios usando 120 máquinas virtuales con un índice de lectura/escritura de 70:30 y un tamaño de bloque de 64K en un clúster de vSAN de cuatro hosts basado íntegramente en tecnología flash reveló una carga desequilibrada en todas las NIC.

Los gráficos de rendimiento de vSphere muestran una carga desequilibrada en las NIC.

### Pérdida de redundancia de vínculo superior de red

Considere un error de red introducido en esta configuración. vmnic1 está deshabilitado en un determinado host de vSAN. Como resultado, se ve afectado el puerto **vmk2**. Una NIC con errores activa tanto alarmas de conectividad de red como alarmas de redundancia.

Para vSAN, este proceso de conmutación por error se activa aproximadamente **10 segundos** después de que CMMDS detecta un error . Durante la conmutación por error y la recuperación, vSAN detiene las conexiones activas en la red con errores e intenta restablecer las conexiones en la red funcional restante.

Debido a que dos puertos de VMkernel de vSAN independientes se comunican en VLAN aisladas, es posible que se activen errores de comprobación de estado de vSAN. Esto se espera, ya que **vmk2** ya no puede comunicarse con sus pares en VLAN 3265.

Los gráficos de rendimiento muestran que la carga de trabajo afectada se reinició en vmnic0, ya que vmnic1 tiene un error (deshabilitado para los fines de esta prueba). Esta prueba ilustra una diferencia importante entre la formación de equipos de NIC de vSphere y esta topología. vSAN intenta restablecer o reiniciar las conexiones en la red restante.

Sin embargo, en algunos casos de error, la recuperación de las conexiones afectadas puede requerir hasta **90 segundos** para completarse debido al tiempo de espera de la conexión TCP de ESXi. Es posible que se produzca un error en los intentos de conexión posteriores, pero el tiempo de espera de los intentos de conexión se agota en 5 segundos y los intentos se rotan en todas las direcciones IP posibles. Este comportamiento puede afectar a la E/S del invitado de la máquina virtual. Como resultado, es posible que sea necesario volver a intentar la E/S de las máquinas virtuales y las aplicaciones.

Por ejemplo, en las máquinas virtuales con Windows Server 2012, es posible que se registren los identificadores de eventos 153 (restablecimiento de dispositivos) y 129 (eventos de reintento) durante el proceso de conmutación por error y recuperación. En el ejemplo, el identificador de evento 129 se registró aproximadamente 90 segundos hasta que se recuperó la E/S.

Es posible que tenga que modificar la configuración del tiempo de espera del disco de algunos sistemas operativos invitados para garantizar que no se vean gravemente afectados. Los valores de tiempo de espera de disco pueden variar en función de la presencia de VMware Tools y del tipo de sistema operativo invitado y su versión. Para obtener más información sobre cómo cambiar los valores de tiempo de espera del disco de SO invitado, consulte el artículo 1009465 de la base de conocimientos de VMware.

### Recuperación y conmutación por recuperación

Cuando se repara la red, las cargas de trabajo no se vuelven a equilibrar automáticamente, a menos que se produzca otro error al forzar la carga de trabajo debido a otro error. Tan pronto como la red afectada se recupera, queda disponible para las nuevas conexiones TCP.

## Configuración 3: LACP dinámico

Puede configurar un canal de puerto LACP de dos puertos en un conmutador y un grupo de adición de dos vínculos superiores en un vSphere Distributed Switch.

En este ejemplo, utilice redes de 10 GB con dos vínculos superiores físicos por servidor.

**Nota** vSAN a través de RDMA no admite esta configuración.

## Configurar un conmutador de red

Configure el vSphere Distributed Switch con los siguientes ajustes.

- Identifique los puertos en cuestión en los que se conectará el host vSAN.
- Cree un canal de puerto.
- Si utiliza redes VLAN, establezca un enlace troncal de la VLAN correcta al canal del puerto.
- Configure las opciones de distribución o equilibrio de carga (hash).
- Establezca el modo LACP en activo/dinámico.
- Verifique la configuración de MTU.

## Configurar vSphere

Configure la red de vSphere con la siguiente configuración.

- Configure vDS con la MTU correcta.
- Agregue hosts a vDS.
- Cree un LAG con el número correcto de vínculos superiores y los mismos atributos que el canal de puerto.
- Asigne vínculos superiores físicos al LAG.
- Cree un grupo de puertos distribuidos para el tráfico de vSAN y asigne la VLAN correcta.
- Configure los puertos de VMkernel para vSAN con la MTU correcta.

## Configurar el conmutador físico

Configure el conmutador físico con la siguiente configuración. Para obtener más información sobre cómo establecer esta configuración en los servidores Dell, consulte: http://www.dell.com/Support/Article/es/es/19/HOW10364.

Configurar un LAG de dos vínculos superiores:

- Use los puertos de conmutador 36 y 18.
- Esta configuración utiliza el enlace troncal de VLAN, por lo que el canal de puerto se encuentra en modo troncal de VLAN, con el enlace troncal de las VLAN adecuadas.
- Utilice el siguiente método para el equilibrio de carga o la distribución de la carga: **direcciones IP de origen y destino, puerto TCP/UDP y VLAN**
- Compruebe que el modo LACP sea **Activo** (Dinámico).

Utilice los siguientes comandos para configurar un canal de puerto individual en un conmutador Dell:

- Cree un canal de puerto.

```
#interface port-channel 1
```

- Establezca el canal de puerto en modo troncal de VLAN.

```
#switchport mode trunk
```

- Permita el acceso a la red VLAN.

```
#switchport trunk allowed vlan 3262
```

- Configure la opción de equilibrio de carga.

```
#hashing-mode 6
```

- Asigne los puertos correctos al canal de puerto y establezca el modo Activo.
- Compruebe que el canal de puerto esté configurado correctamente.

```
#show interfaces port-channel 1


Channel Ports Ch-Type Hash Type Min-links Local Prf

------- ----------------------------- -------- --------- --------- ---------

Po1 Active: Te1/0/36, Te1/0/18 Dynamic 6 1 Disabled

Hash Algorithm Type

1 - Source MAC, VLAN, EtherType, source module and port Id

2 - Destination MAC, VLAN, EtherType, source module and port Id

3 - Source IP and source TCP/UDP port

4 - Destination IP and destination TCP/UDP port

5 - Source/Destination MAC, VLAN, EtherType, source MODID/port

6 - Source/Destination IP and source/destination TCP/UDP port

7 - Enhanced hashing mode
```

```
#interface range Te1/0/36, Te1/0/18

#channel-group 1 mode active
```

Configuración completa:

```
#interface port-channel 1

#switchport mode trunk

#switchport trunk allowed vlan 3262
```

```
#hashing-mode 6

#exit

#interface range Te1/0/36,Te1/018

#channel-group 1 mode active

#show interfaces port-channel 1
```

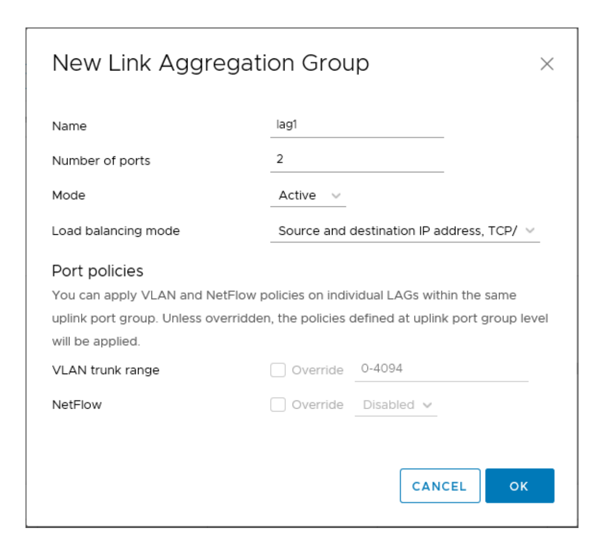
**Nota** Repita este procedimiento en todos los puertos del conmutador participante que estén conectados a los hosts vSAN.

## Configurar vSphere Distributed Switch

Antes de comenzar, asegúrese de que vDS esté actualizado a una versión que admita LACP. Para comprobarlo, haga clic con el botón derecho en el vDS y compruebe si la opción de actualización está disponible. Es posible que tenga que actualizar el vDS a una versión que admita LACP.

## Crear un LAG en vDS

Para crear un LAG en un conmutador distribuido, seleccione el vDS, haga clic en la pestaña **Configurar** y seleccione **LACP**. Agregue un nuevo LAG.




Configure el LAG con las siguientes propiedades:

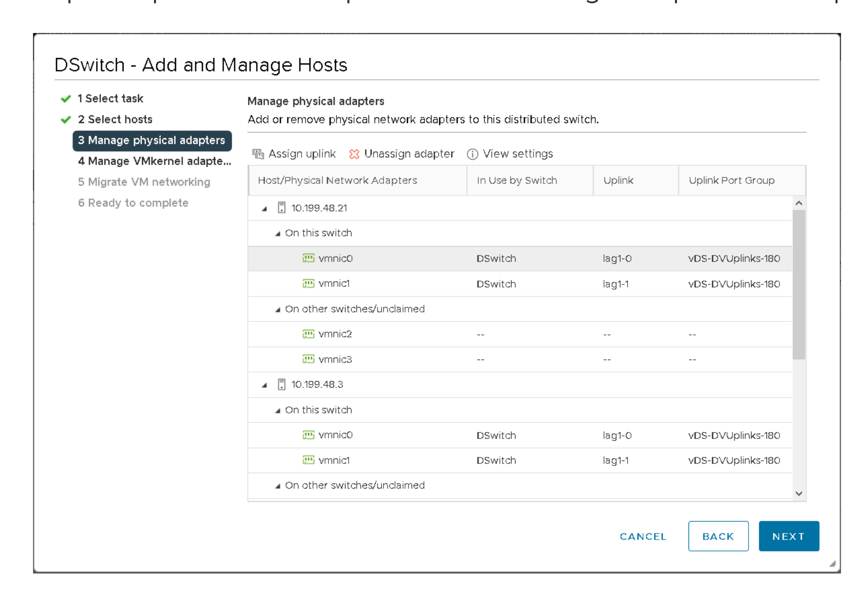
- Nombre de LAG: **lag1**
- Número de puertos: **2** (para que coincida con el canal del puerto en el conmutador)
- Modo: **Activo**, para que coincida con el conmutador físico.
- Modo de equilibrio de carga: **direcciones IP de origen y destino, puerto TCP/UDP y VLAN**

## Agregar vínculos superiores físicos a un LAG

Se agregaron hosts vSAN al vDS. Asigne cada vmnic a los puertos de LAG adecuados.

- Haga clic con el botón derecho en el vDS y seleccione **Agregar y administrar hosts...**
- Seleccione **Administrar redes de host** y agregue los hosts asociados.
- En **Administrar adaptadores físicos**, seleccione los adaptadores adecuados y asígnelos al puerto LAG.
- Migre vmnic0 desde la posición de vínculo superior 1 al puerto 0 de LAG1.

Repita el procedimiento para vmnic1 a la segunda posición del puerto de LAG, lag1-1.




## Configurar la directiva de formación de equipos y conmutación por error de grupos de puertos distribuidos

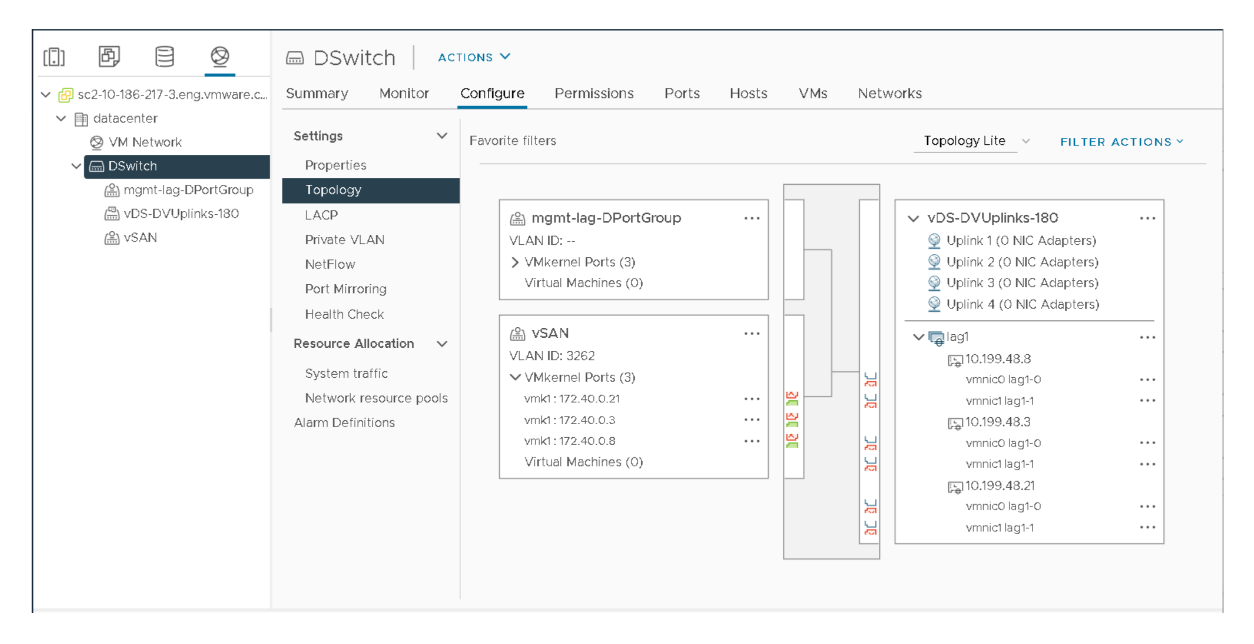
Asigne el grupo LAG como un **Vínculo superior activo** en la directiva de formación de equipos y conmutación por error del grupo de puertos distribuidos. Seleccione o cree el grupo de puertos distribuidos designados para el tráfico de vSAN. Esta configuración utiliza un grupo de puertos de vSAN llamado **vSAN** con el identificador de VLAN 3262 etiquetado. Edite el grupo de puertos y configure la directiva de formación de equipos y conmutación por error para reflejar la nueva configuración de LAG.

Asegúrese de que el grupo LAG **lag1** esté en la posición de vínculos superiores activos y compruebe que los vínculos superiores restantes se encuentren en la posición **Sin utilizar**.

**Nota** Cuando se selecciona un grupo de adición de enlaces (LAG) como el único vínculo superior activo, el modo de equilibrio de carga del LAG anula el modo de equilibrio de carga del grupo de puertos. Por lo tanto, la siguiente directiva no desempeña ninguna función: **Enrutar según el puerto virtual de origen**.

## Crear las interfaces de VMkernel

El paso final es crear las interfaces de VMkernel para utilizar el nuevo grupo de puertos distribuidos, lo que garantiza que se etiqueten para el tráfico de vSAN. Observe que cada vmknic de vSAN se puede comunicar a través de vmnic0 y vmnic1 en un grupo de LAG para proporcionar equilibrio de carga y conmutación por error.




## Configurar el equilibrio de carga

Desde una perspectiva de equilibrio de carga, no existe ningún equilibrio coherente entre todos los hosts de todos los vmnics de esta configuración de LAG, pero existe una mayor coherencia en comparación con la directiva **Enrutar según la carga de la NIC física** que se utiliza en la Configuración 1 y el método de aislamiento/varios vmknics que se utiliza en la Configuración 2.

El gráfico de rendimiento vSphere de los hosts individuales muestra un equilibrio de carga mejorado.

## Pérdida de redundancia de vínculo superior de red

Cuando vmnic1 está deshabilitado en un determinado host de vSAN, se activa una alarma de redundancia de red.

No se activa ninguna alarma de estado de vSAN, y el impacto en la E/S de invitado es mínimo en comparación con la configuración con aislamiento de varios vmknics. Esta configuración no tiene que detener ninguna sesión TCP con LACP configurado.

## Recuperación y conmutación por recuperación

En un escenario de conmutación por recuperación, el comportamiento es diferente entre la formación de equipos basada en carga, varios vmknics y LACP en un entorno vSAN. Después de la recuperación de vmnic1, el tráfico se equilibra automáticamente en ambos vínculos superiores activos. Este comportamiento puede favorecer el tráfico de vSAN.

### ¿Configurar la conmutación por recuperación en Sí o en No?

Una directiva de equilibrio de carga de LAG reemplaza la directiva de formación de equipos y conmutación por error para grupos de puertos distribuidos de vSphere. Tenga en cuenta también las instrucciones sobre el valor de la conmutación por recuperación. Las pruebas de laboratorio no muestran las diferencias de comportamiento discernible entre ajustar la conmutación por recuperación en **Sí** o en **No** con LACP. La configuración de LAG tiene prioridad sobre la configuración del grupo de puertos.

**Nota** Los valores de detección de errores de red se mantienen como **Solo estado de vínculo**, ya que el sondeo de señal no es compatible con LACP. Consulte el artículo de la base de conocimientos de VMware sobre el equilibrio de carga de hash de IP (2006129)

## Configuración 4: LACP estático – Enrutar según el hash de IP

Puede utilizar un canal de puerto estático LACP de dos puertos en un conmutador y dos vínculos superiores activos en un conmutador estándar de vSphere.

En esta configuración, utilice redes de 10 GB con dos vínculos superiores físicos por servidor. Existe una única interfaz de VMkernel (vmknic) para vSAN en cada host.

Para obtener más información sobre los requisitos de host y ejemplos de configuración, consulte los siguientes artículos de la base de conocimientos de VMware:

- Requisitos del host ESX/ESXi para la adición de enlaces (1001938)
- Configuración de muestra de EtherChannel/Protocolo de control de adición de enlaces (LACP) con conmutadores ESXi/ESX y Cisco/HP (1004048)

**Nota** vSAN a través de RDMA no admite esta configuración.

### Configurar un conmutador físico

Configure un canal de puerto estático de dos vínculos ascendentes siguiendo estos pasos:

- Puertos del conmutador 43 y 44
- Enlace troncal de VLAN, por lo que el canal de puerto se encuentra en modo troncal de VLAN, con el enlace troncal de las VLAN adecuadas.
- No especifique la directiva de equilibrio de carga en el grupo del canal de puerto.

Siga estos pasos para configurar un canal de puerto individual en el conmutador:

Paso 1: Cree un canal de puerto.

```
#interface port-channel 13
```

Paso 2: Establezca el canal de puerto en modo troncal de VLAN.

```
#switchport mode trunk
```

Paso 3: Permita las VLAN adecuadas.

```
#switchport trunk allowed vlan 3266
```

Paso 4: Asigne los puertos correctos al canal de puerto y establezca el modo en Activo.

```
#interface range Te1/0/43, Te1/0/44

#channel-group 1 mode on
```

Paso 5: Compruebe que el canal de puerto esté configurado como estático.

```
#show interfaces port-channel 13


Channel Ports Ch-Type Hash Type Min-links Local Prf

------- ----------------------------- -------- --------- --------- --

Po13 Active: Te1/0/43, Te1/0/44 Static 7 1 Disabled

Hash Algorithm Type

1 - Source MAC, VLAN, EtherType, source module and port Id

2 - Destination MAC, VLAN, EtherType, source module and port Id

3 - Source IP and source TCP/UDP port

4 - Destination IP and destination TCP/UDP port

5 - Source/Destination MAC, VLAN, EtherType, source MODID/port

6 - Source/Destination IP and source/destination TCP/UDP port

7 - Enhanced hashing mode
```

## Configurar un conmutador estándar de vSphere

En este ejemplo, asumiremos que sabe cómo configurar y crear conmutadores estándar de vSphere.

En este ejemplo se utiliza la siguiente configuración:

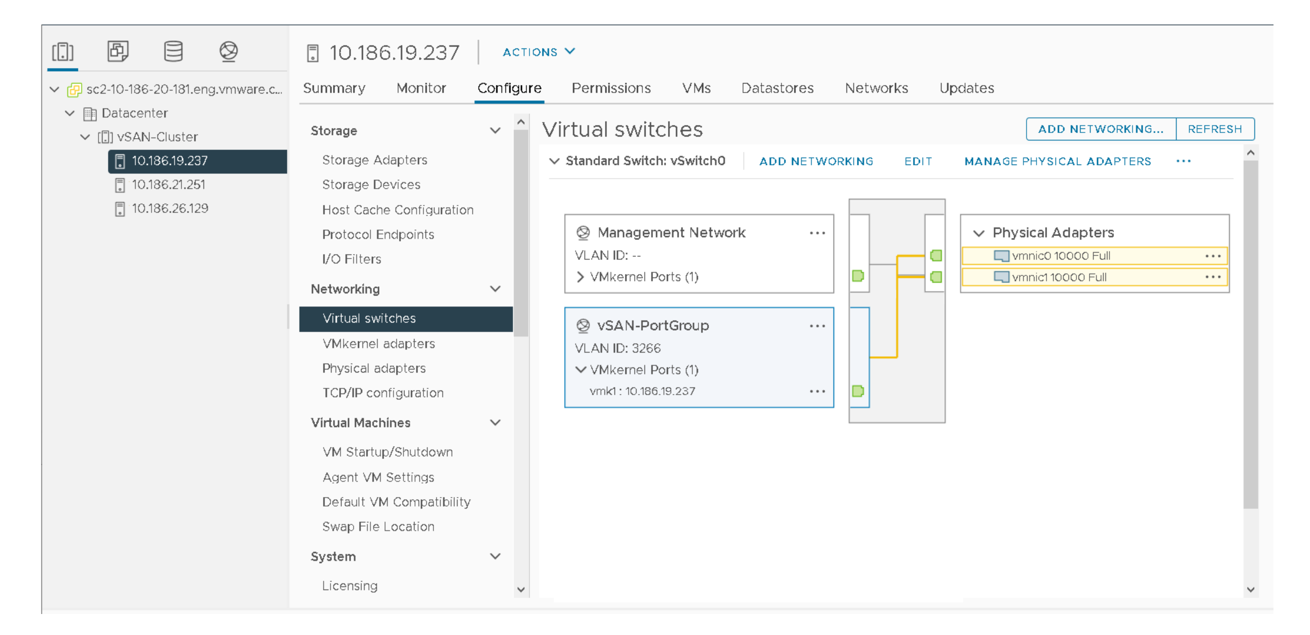
- Hosts de vSAN idénticos
- Vínculos superiores llamados vmnic0 y vmnic1
- VLAN 3266 con enlace troncal a los puertos del conmutador y al canal de puerto
- Tramas gigantes

En cada host, cree **vSwitch1** con la MTU configurada en 9000, y vmnic0 y vmnic1 agregados al vSwitch. En la directiva de formación de equipos y conmutación por error, establezca los dos adaptadores en la posición **Activo**. Establezca la directiva de equilibrio de carga en **Enrutar según el hash de IP**.

Configure la formación de equipos y la conmutación por error del grupo de puertos distribuidos para el tráfico de vSAN siguiendo estos pasos:

- Directiva de equilibrio de carga: **Enrutar según el hash de IP**.
- Detección de errores de red: **Solo estado de vínculo**.
- Notificar a conmutadores: **Sí**.
- Conmutación por recuperación: **Sí**.
- Asegúrese de que los dos vínculos superiores se encuentren en la posición **Vínculos superiores activos**.

Utilice los valores predeterminados para la detección de redes, la notificación a conmutadores y la conmutación por recuperación. Todos los grupos de puertos heredan la directiva de formación de equipos y conmutación por error que se estableció en el nivel de vSwitch. Puede anular las directivas de conmutación por error y formación de equipos de grupos de puertos individualmente para que difieran del vSwitch principal, pero asegúrese de usar el mismo conjunto de vínculos superiores para el equilibrio de carga de hash de IP en todos los grupos de puertos.




## Configurar el equilibrio de carga

Aunque se utilizan ambos vínculos superiores físicos, no existe un equilibrio de tráfico coherente en todos los vmnics físicos. La figura muestra que solo el tráfico activo es tráfico de vSAN, que esencialmente era de cuatro vmknics o direcciones IP. Este comportamiento puede deberse a la escasa cantidad de direcciones IP y a posibles hashes. Sin embargo, en algunos casos, es posible que el conmutador virtual pase el tráfico de forma coherente a través de un vínculo superior en el equipo. Para obtener más información sobre el algoritmo de hash de IP, consulte la documentación oficial de vSphere sobre *Enrutar según el hash de IP*.

## Redundancia de red

En este ejemplo, vmnic1 está conectado a un puerto que se ha deshabilitado del conmutador para centrarse en el comportamiento de errores y redundancia. Tenga en cuenta que se ha activado una alarma de redundancia de vínculo superior de red.

No se activaron alarmas de estado de vSAN. Los componentes del clúster y de la máquina virtual no se ven afectados y este error no interrumpe la E/S de almacenamiento invitado.

## Recuperación y conmutación por recuperación

Una vez que vmnic1 se recupera, el tráfico se equilibra automáticamente en ambos vínculos superiores activos.

# Network I/O Control

11

Utilice vSphere Network I/O Control para establecer niveles de calidad de servicio (QoS) en el tráfico de red.

vSphere Network I/O Control es una función disponible con conmutadores distribuidos de vSphere. Utilícelo para implementar la calidad de servicio (QoS) en el tráfico de red. Esto puede ser útil para vSAN cuando el tráfico de vSAN debe compartir la NIC física con otros tipos de tráfico, como vMotion, administración y máquinas virtuales.

## Reservas, recursos compartidos y límites

Puede configurar una **reserva** para que Network I/O Control garantice que el ancho de banda mínimo esté disponible en el adaptador físico para vSAN.

Las reservas pueden ser útiles cuando el tráfico *en ráfagas*, como vMotion o la evacuación de hosts completos, afecta al tráfico de vSAN. Las reservas solo se invocan si hay contención de ancho de banda de red. Una desventaja de las reservas en Network I/O Control es que el ancho de banda de reserva no utilizado no se puede asignar al tráfico de la máquina virtual. El total de ancho de banda reservado entre todos los tipos de tráfico de sistema no puede superar el 75 % del ancho de banda proporcionado por el adaptador de red físico de menor capacidad.

**Prácticas recomendadas de vSAN sobre las reservas**. El tráfico reservado para vSAN no se pueda asignar al tráfico de la máquina virtual, por lo que evite el uso de reservas de NIOC en entornos de vSAN.

La configuración de **recursos compartidos** pone un ancho de banda disponible para vSAN cuando el adaptador físico asignado para vSAN se satura. Esto evita que vSAN consuma toda la capacidad del adaptador físico durante las operaciones de reconstrucción y sincronización. Por ejemplo, es posible que el adaptador físico se sature cuando se produce un error en otro adaptador físico del equipo y todo el tráfico del grupo de puertos se transfiere a otros adaptadores del equipo. La opción de **recursos compartidos** garantiza que ningún otro tráfico afecte a la red de vSAN.

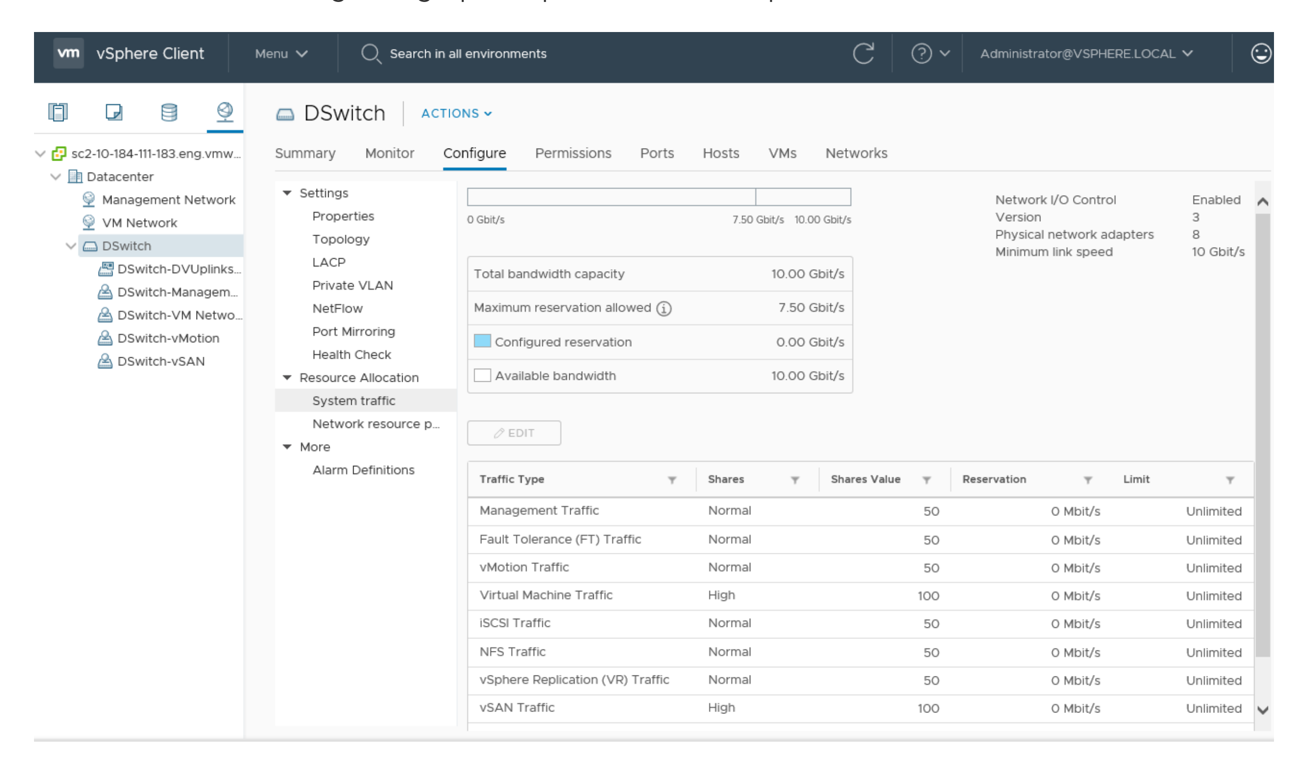
**Recomendación de vSAN sobre recursos compartidos**. Esta es la más equitativa de las técnicas de asignación de ancho de banda de NIOC. Esta técnica es idónea para entornos de vSAN.

La configuración de **límites** define el ancho de banda máximo que puede consumir un determinado tipo de tráfico en un adaptador. Si ningún otro está utilizando el ancho de banda adicional, el tipo de tráfico con el límite tampoco podrá consumirlo.

**Recomendación de vSAN sobre límites**. Dado que los tipos de tráfico con límites no pueden consumir ancho de banda adicional, evite usar límites de NIOC en entornos de vSAN.

## Grupos de recursos de red

Puede ver todos los tipos de tráfico del sistema que pueden controlarse con Network I/O Control. Si tiene varias redes de máquinas virtuales, puede asignar cierta cantidad de ancho de banda al tráfico de la máquina virtual. Use grupos de recursos de red para consumir partes de ese ancho de banda según el grupo de puertos de la máquina virtual.




## Habilitar Network I/O Control

Puede habilitar Network I/O Control en las propiedades de configuración de vDS. Haga clic con el botón derecho en el vDS de vSphere Client y seleccione el menú **Configuración > Editar configuración**.

**Nota** Network I/O Control solo está disponible en conmutadores distribuidos de vSphere, no en los vSwitch estándar.

Puede utilizar Network I/O Control para reservar ancho de banda para el tráfico de red en función de la capacidad de los adaptadores físicos en un host. Por ejemplo, si el tráfico de vSAN utiliza adaptadores de red físicos de 10 GbE y estos se comparten con otros tipos de tráfico del sistema, puede utilizar vSphere Network I/O Control para garantizar una cierta cantidad de ancho de banda para vSAN. Esto puede resultar útil cuando el tráfico como vSphere vMotion, vSphere HA y el tráfico de las máquinas virtuales comparten la misma NIC física que la red de vSAN.

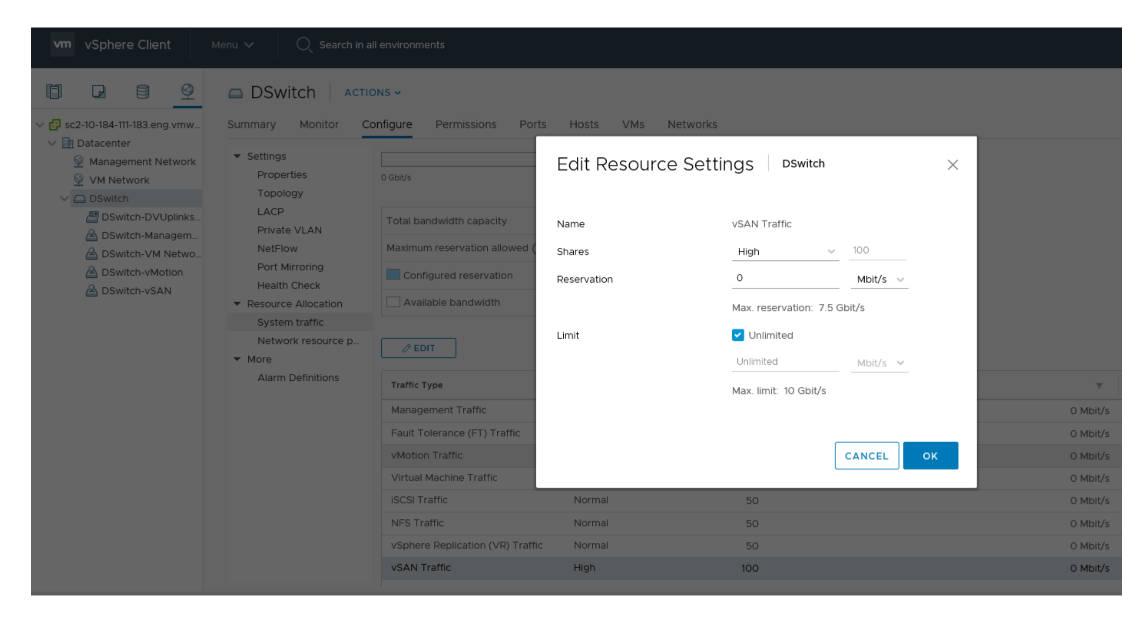
Este capítulo incluye los siguientes temas:

- Ejemplo de configuración de Network I/O Control

# Ejemplo de configuración de Network I/O Control

Puede configurar Network I/O Control para un clúster de vSAN.

Considere un clúster de vSAN con un solo adaptador físico de 10 GbE. Esta NIC controla el tráfico de vSAN, vSphere vMotion y las máquinas virtuales. Para cambiar el valor de los recursos compartidos de un tipo de tráfico, seleccione ese tipo de tráfico en la vista Tráfico del sistema (**VDS > Configurar > Asignación de recursos > Tráfico del sistema**) y haga clic en **Editar**. El valor de los recursos compartidos del tráfico de vSAN se cambió de los valores predeterminados de Normal/50 a Alto/100.




Edite el resto de tipos de tráfico para que coincidan con los valores de recursos compartidos mostrados en la tabla.

### Tabla 11-1. Configuración de NIOC de ejemplo

| Tipo de tráfico | Recursos compartidos | Valor |
| --- | --- | --- |
| **vSAN** | Alto | 100 |
| **vSphere vMotion** | Bajo | 25 |
| **Máquina virtual** | Normal | 50 |
| **iSCSI/NFS** | Bajo | 25 |

Si el adaptador de 10 GbE se satura, Network I/O Control asignará 5 Gbps a vSAN en el adaptador físico, 3,5 Gbps al tráfico de la máquina virtual y 1,5 Gbps a vMotion. Utilice estos valores como punto de partida para establecer la configuración de NIOC en la red de vSAN. Asegúrese de que vSAN tenga la prioridad más alta de cualquier protocolo.

Para obtener más información sobre los distintos parámetros de asignación de ancho de banda, consulte el documento *Redes de vSphere* .

Con cada una de las ediciones de vSphere para vSAN, VMware proporciona un conmutador distribuido de vSphere como parte de la edición. Network I/O Control puede configurarse con cualquier edición de vSAN.

# Información sobre las topologías de red de vSAN 12

La arquitectura de vSAN admite diferentes topologías de red. Estas topologías afectan a la implementación general y a la administración de vSAN.

La introducción de la compatibilidad con unidifusión en vSAN 6.6 simplifica el diseño de la red.

Este capítulo incluye los siguientes temas:



## Implementaciones estándar

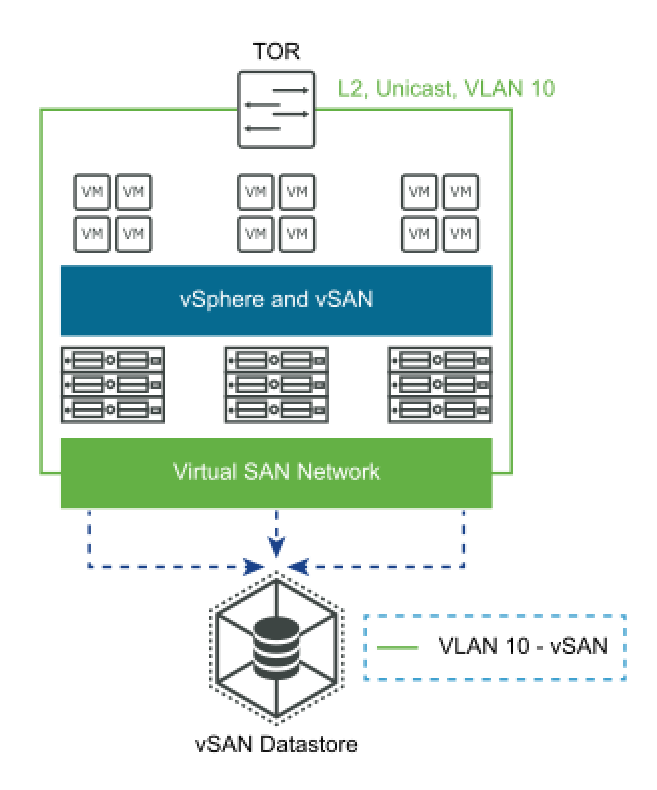
vSAN admite varios tipos de implementación de sitio único.

### Capa 2, un solo sitio y un solo bastidor

Esta topología de red es responsable de reenviar paquetes a través de dispositivos intermedios de capa 2, como hosts, puentes o conmutadores.

La topología de red de capa 2 ofrece la implementación y la administración más sencilla de vSAN. VMware recomienda el uso y la configuración de la intromisión IGMP para evitar el envío de tráfico de multidifusión innecesario en la red. En este primer ejemplo, estamos buscando un único sitio y quizás incluso un único bastidor de servidores que utilicen vSAN 6.5 o una versión anterior. Esta versión utiliza multidifusión, por lo que debe habilitar la intromisión IGMP. Dado que todo está en la misma capa 2, no es necesario configurar el enrutamiento para el tráfico de multidifusión.

Las implementaciones de capa 2 se simplifican aún más con vSAN 6.6 y versiones posteriores, lo que introduce compatibilidad con unidifusión. No se requiere la intromisión de IGMP.



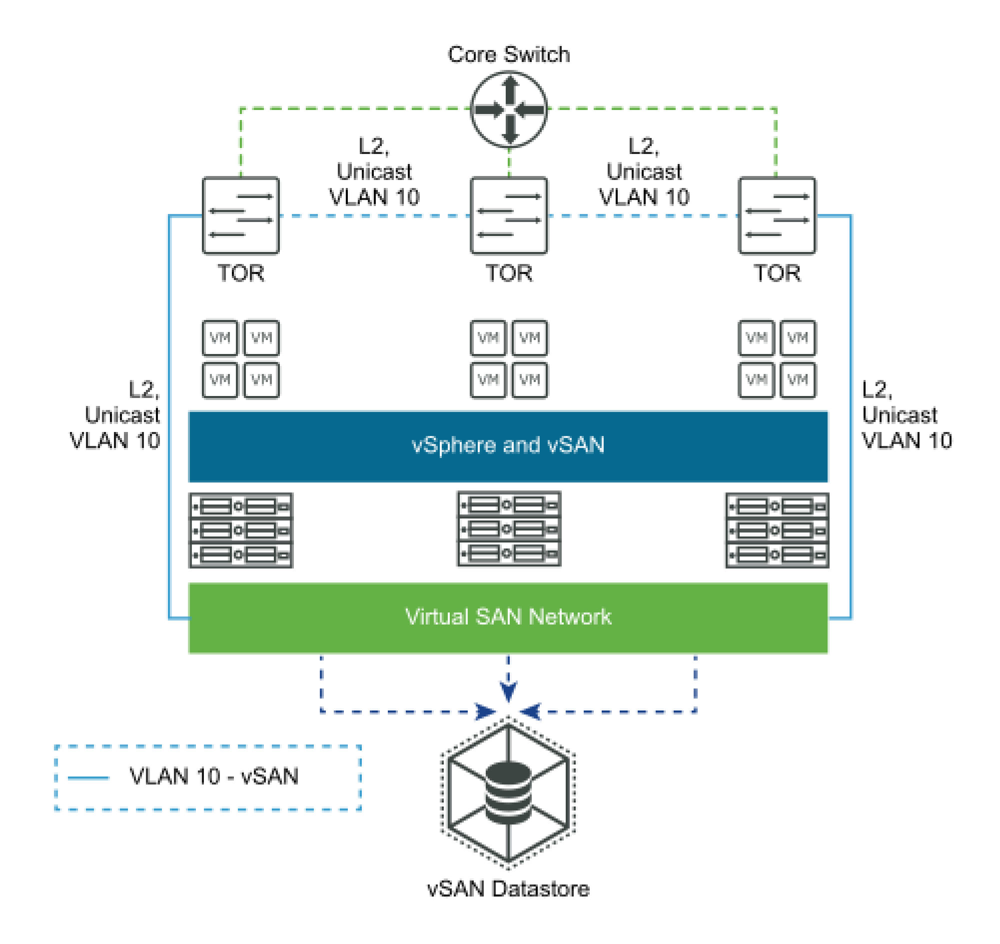

## Capa 2, sitio único y varios bastidores

Esta topología de red funciona con la implementación de la capa 2 en la que hay varios bastidores y varios conmutadores en parte superior del bastidor (TOR) conectados a un conmutador principal.

En las siguientes figuras, la línea de puntos azules entre los TOR muestra que la red de vSAN está disponible y es accesible para todos los hosts del clúster de vSAN. Sin embargo, los hosts de los diferentes bastidores se comunican entre sí a través de la capa 3, lo que implica el uso de PIM para enrutar el tráfico multidifusión entre los hosts. Los TOR no están físicamente conectados entre sí.

VMware recomienda que todos los TOR estén configurados para la intromisión IGMP con el fin de evitar el tráfico de multidifusión innecesario en la red. Debido a que no hay enrutamiento del tráfico, no es necesario configurar PIM para que enrute el tráfico de multidifusión.

Esta implementación es más sencilla en vSAN 6.6 y versiones posteriores, ya que el tráfico de vSAN es de unidifusión. Con el tráfico de unidifusión, no es necesario configurar la intromisión IGMP en los conmutadores.




## Capa 3, sitio único y varios bastidores

Esta topología de red funciona para implementaciones de vSAN en las que se utiliza la capa 3 para enrutar el tráfico de vSAN.

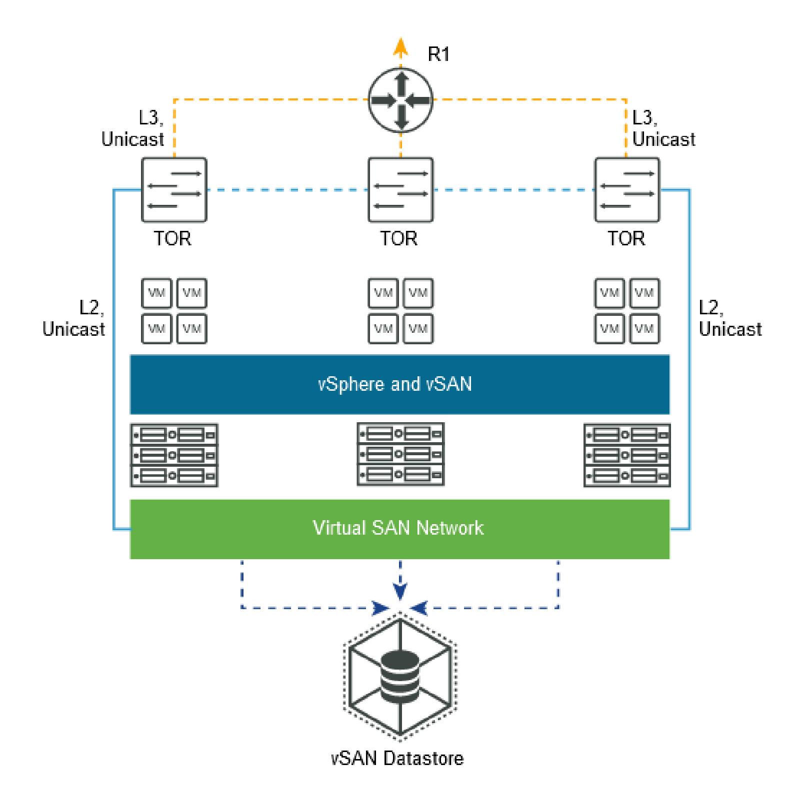
Esta topología de red simple de capa 3 utiliza varios bastidores en el mismo centro de datos, cada uno con su propio conmutador TOR. Enrute la red de vSAN entre los diferentes bastidores de capa 3 para permitir que todos los hosts del clúster de vSAN se comuniquen. Coloque los puertos de VMkernel de vSAN en diferentes subredes o VLANs, y utilice una subred o VLAN independiente para cada bastidor.

Esta topología de red enruta los paquetes a través de dispositivos intermedios compatibles con la capa 3, como los enrutadores y los conmutadores compatibles con la capa 3. Cuando los hosts se implementan en diferentes segmentos de red de capa 3, el resultado es una topología de red enrutada.

Con vSAN 6.5 y versiones anteriores, VMware recomienda el uso y la configuración de la intromisión IGMP, ya que estas implementaciones requieren multidifusión. Configure PIM en los conmutadores físicos para facilitar el enrutamiento del tráfico de multidifusión.

vSAN 6.6 y versiones posteriores simplifican esta topología. Debido a que no hay tráfico de multidifusión, no es necesario configurar la intromisión IGMP. No es necesario configurar PIM para enrutar el tráfico de multidifusión.

A continuación, se ofrece una descripción general de un ejemplo de implementación de vSAN 6.6 a través de capa 3. No hay ningún requisito para la intromisión IGMP o PIM, ya que no hay tráfico de multidifusión.




# Implementaciones de clúster ampliado

vSAN es compatible con las implementaciones de clúster ampliado que abarcan dos ubicaciones.

En vSAN 6.5 y versiones anteriores, el tráfico de vSAN entre sitios de datos es de **multidifusión** para los metadatos y de **unidifusión** para las operaciones de E/S.

En vSAN 6.6 y versiones posteriores, todo el tráfico es de **unidifusión**. En todas las versiones de vSAN, el tráfico testigo entre un sitio de datos y el host testigo es de unidifusión.

## Capa 2 en todos los sitios

Puede configurar un clúster ampliado de vSAN en una red de capa 2, pero no se recomienda esta configuración.

Considere un diseño en el que el clúster ampliado de vSAN esté configurado en un diseño de capa 2 grande. Los sitios de datos 1 y 2 son donde se implementan las máquinas virtuales. El sitio 3 contiene el host testigo.

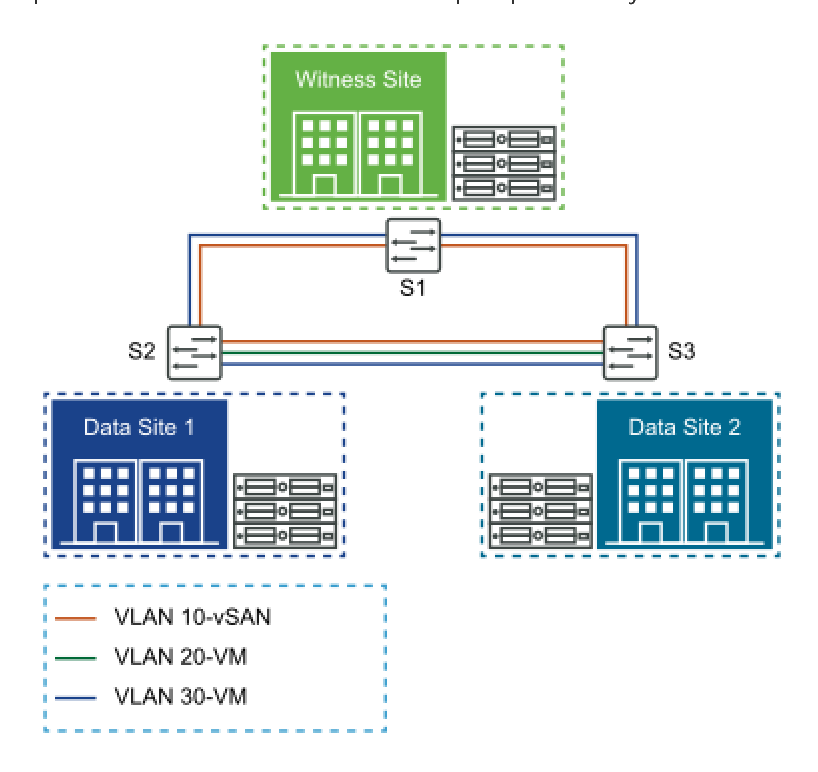
**Nota** Para obtener los mejores resultados, no utilice una red de capa 2 ampliada en todos los sitios.

Para demostrar la capa 2 en todos los sitios de la forma más simple posible, utilizamos conmutadores (y no enrutadores) en las topologías.

Las redes de capa 2 no pueden tener bucles (varias rutas de acceso), por lo que se necesitan funciones como el protocolo de árbol de expansión (Spanning Tree Protocol, STP) para bloquear una de las conexiones entre el sitio 1 y el sitio 2. Ahora, suponga una situación en la que el vínculo entre el sitio 2 y el sitio 3 esté roto (el vínculo entre el sitio 1 y el sitio 2). El tráfico de red ahora se puede cambiar del sitio 1 al sitio 2 a través del host testigo del sitio 3. Como VMware admite un ancho de banda mucho menor y una latencia mucho mayor para el host testigo, se observa una disminución significativa del rendimiento si el tráfico de red de datos pasa a través de un sitio testigo de especificación más bajo.

Si el tráfico de conmutación entre sitios de datos a través del sitio testigo no afecta a la latencia de las aplicaciones y el ancho de banda es aceptable, se permite una configuración de capa 2 ampliada entre sitios. En la mayoría de los casos, una configuración de este tipo no es factible y agrega complejidad a los requisitos de red.

Con vSAN 6.5 o una versión anterior, que utiliza tráfico de multidifusión, debe configurar la intromisión IGMP en los conmutadores. Esto no es necesario con vSAN 6.6 y versiones posteriores. PIM no es necesario porque no hay enrutamiento de tráfico de multidifusión.




## Configuraciones de clúster ampliado admitidas

vSAN admite configuraciones de clúster ampliado.

La siguiente configuración evita que el tráfico del sitio 1 se enrute al sitio 2 a través del host testigo, en caso de que se produzca un error en cualquiera de las redes de los sitios de datos. Esta configuración evita la degradación del rendimiento. Para asegurarse de que el tráfico de datos no se conmuta a través del host testigo, use la siguiente topología de red.

Entre el sitio 1 y el sitio 2, implemente una configuración de capa 2 con conmutador ampliado o una configuración de capa 3 enrutada. Ambas configuraciones están admitidas.

Entre el sitio 1 y el host testigo, implemente una configuración de capa 3 enrutada.

Entre el sitio 2 y el host testigo, implemente una configuración de capa 3 enrutada.

Estas configuraciones (L2+L3 y capa 3 en todos los sitios) se describen con las consideraciones que se proporcionan para la multidifusión en vSAN 6.5 y versiones anteriores, y solo para unidifusión, que está disponible en vSAN 6.6. El tráfico de multidifusión introduce pasos de configuración adicionales para la intromisión de IGMP y PIM para enrutar el tráfico de multidifusión.

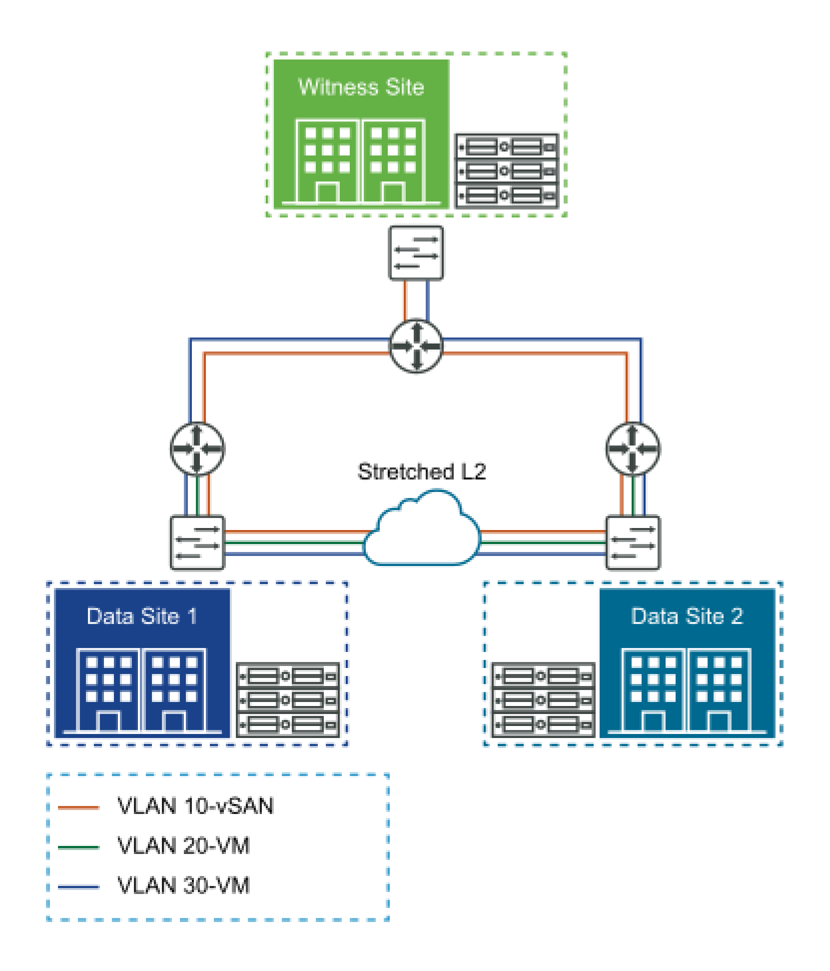
Examinaremos una red de capa 2 ampliada entre los sitios de datos y una red con enrutamiento de capa 3 al sitio testigo. Para demostrar una combinación de capa 2 y capa 3 lo más simple posible, utilice una combinación de conmutadores y enrutadores en las topologías.

## Capa 2 ampliada entre sitios de datos, Capa 3 al host testigo

vSAN admite configuraciones de capa 2 ampliada entre sitios de datos.

El único tráfico que se enruta en este caso es el tráfico testigo. Con vSAN 6.5 y versiones anteriores, que utilizan multidifusión, utilice la intromisión IGMP para el tráfico de multidifusión en vSAN de capa 2 ampliado entre los sitios de datos. Sin embargo, debido a que el tráfico testigo es de unidifusión, no es necesario implementar PIM en los segmentos de capa 3.

Con vSAN 6.6, que utiliza unidifusión, no es necesario tener en cuenta la intromisión IGMP ni PIM.



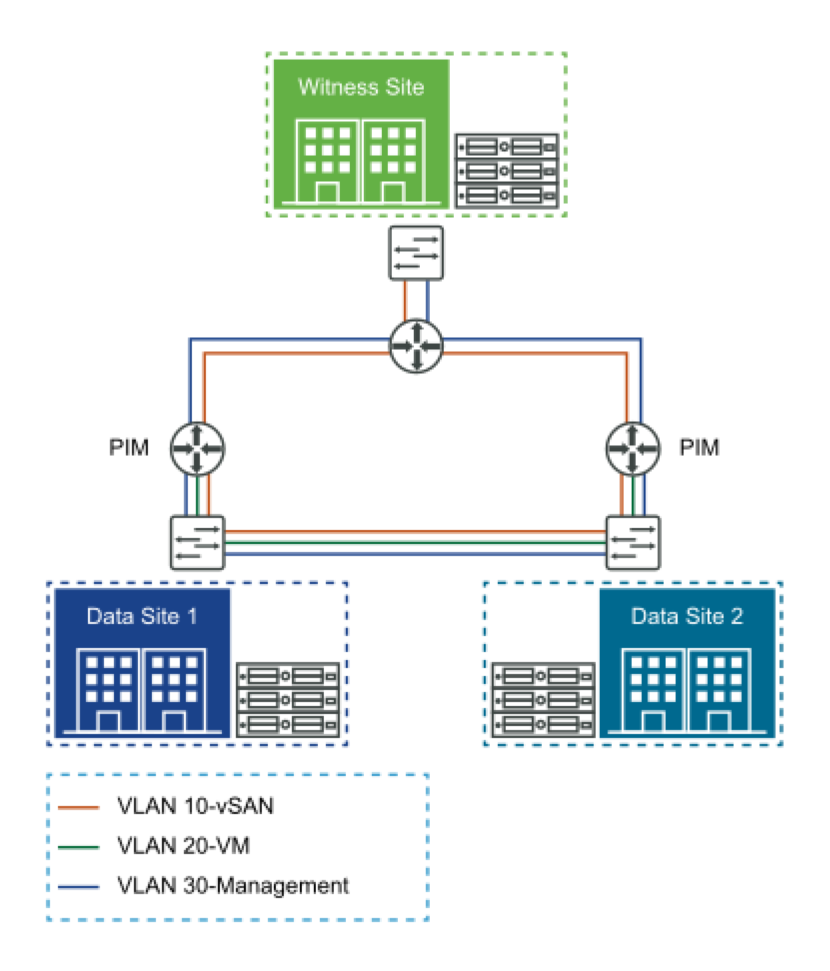

## Capa 3 en todos los sitios

En esta configuración de clúster ampliado de vSAN, el tráfico de datos se enruta entre los sitios de datos y el host testigo.

Para implementar la capa 3 en todos los sitios de la forma más simple posible, utilice enrutadores y conmutadores de enrutamiento en las topologías.

Por ejemplo, supongamos un entorno con vSAN 6.5 o una versión anterior, que utiliza tráfico de multidifusión. En este caso, configure la intromisión de IGMP en los conmutadores del sitio de datos para administrar la cantidad de tráfico de multidifusión en la red. Esto no es necesario en el host testigo, ya que el tráfico testigo es de unidifusión. El tráfico de multidifusión se enruta entre los sitios de datos, por lo que debe configurar PIM para permitir el enrutamiento de multidifusión.

Con vSAN 6.6 y versiones posteriores, no es necesario la intromisión IGMP ni PIM porque todo el tráfico enrutado es de unidifusión.




## Separar el tráfico testigo en los clústeres ampliados de vSAN

vSAN admite la separación del tráfico testigo en los clústeres ampliados.

vSAN 6.5 y versiones posteriores permiten separar el tráfico testigo del tráfico de vSAN en configuraciones de dos nodos. Esto significa que los dos hosts vSAN se pueden conectar directamente sin un conmutador de 10 Gb.

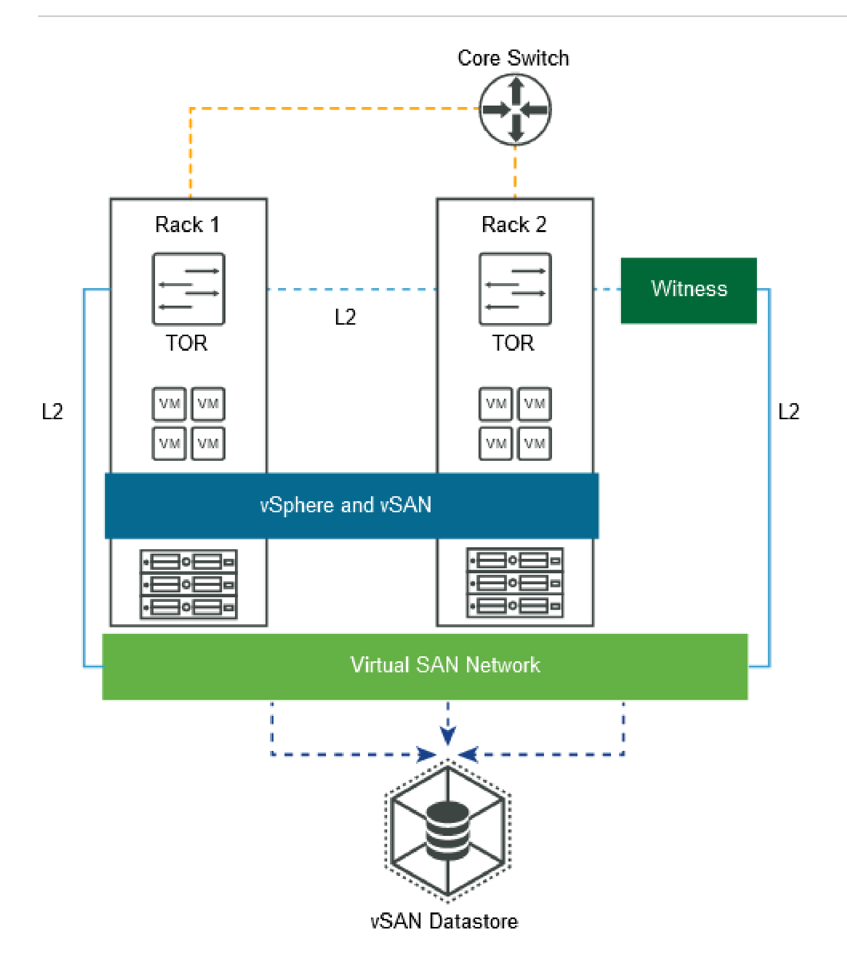
Esta separación de tráfico testigo solo se admite en implementaciones de dos nodos en vSAN 6.6. La separación del tráfico testigo en los clústeres ampliados de vSAN se admite en vSAN 6.7 y versiones posteriores.

## Usar un clúster ampliado para lograr el reconocimiento de los bastidores

Con los clústeres ampliados, vSAN proporciona reconocimiento de los bastidores en un único sitio.

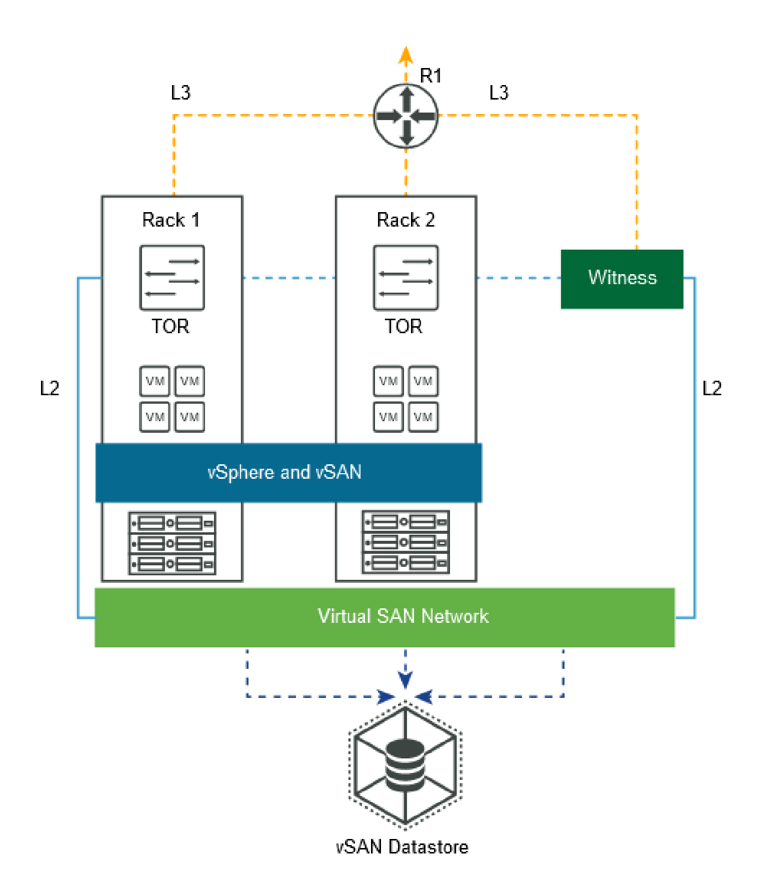
Si tiene dos bastidores de hosts vSAN, puede seguir ejecutando el clúster de vSAN después de un error de bastidor completo. En este caso, la disponibilidad de las cargas de trabajo de la máquina virtual se proporciona mediante el bastidor restante y un host testigo remoto.

**Nota** Para que se admita esta configuración, no coloque el host testigo dentro de los dos bastidores de hosts vSAN.




En este ejemplo, si se produce un error en el bastidor 1, el bastidor 2 y el host testigo proporcionarán la disponibilidad de la máquina virtual. Esta configuración es un entorno previo a vSAN 6.6 y necesita que se configure multidifusión en la red. El host testigo debe estar en la red de vSAN. El tráfico testigo es de unidifusión. En vSAN 6.6 y versiones posteriores, todo el tráfico es de unidifusión.

Esta topología también se admite a través de capa 3. Coloque los puertos de VMkernel de vSAN en diferentes subredes o VLANs, y utilice una subred o VLAN independiente para cada bastidor.




Esta topología admite implementaciones con dos bastidores para lograr el reconocimiento de los bastidores (dominios de errores) con un clúster ampliado de vSAN. Esta solución utiliza un host testigo externo al clúster.

# Implementaciones de vSAN de dos nodos

vSAN admite implementaciones de dos nodos. Las implementaciones de vSAN de dos nodos se utilizan para las oficinas remotas y sucursales (ROBO, Remote Offices/Branch Offices) que tienen una cantidad de cargas de trabajo reducida, pero requieren una alta disponibilidad.

Las implementaciones de vSAN de dos nodos utilizan un tercer host testigo, que puede estar en una ubicación remota de la sucursal. A menudo, el testigo se mantiene en la sucursal, junto con los componentes de administración, como vCenter Server.

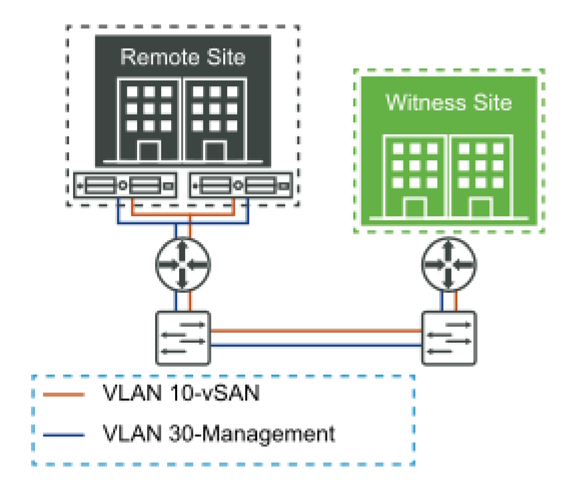
## Versiones de implementación de vSAN de dos nodos anteriores a vSAN 6.5

Las versiones de vSAN anteriores a la 6.5 que admiten implementaciones de dos nodos requieren un conmutador físico en el sitio remoto.

Las redes vSAN de dos nodos más antiguas tienen un requisito para incluir un conmutador físico de 10 GB en el sitio remoto. Si los únicos servidores de este sitio remoto eran los hosts vSAN, esta solución podría no ser eficiente.

Con esta implementación, si no hay otros dispositivos que utilicen el conmutador de 10 Gb, no es necesario tener en cuenta la intromisión de IGMP. Si otros dispositivos del sitio remoto comparten el conmutador de 10 Gb, use la intromisión de IGMP para evitar tráfico de multidifusión excesivo e innecesario.

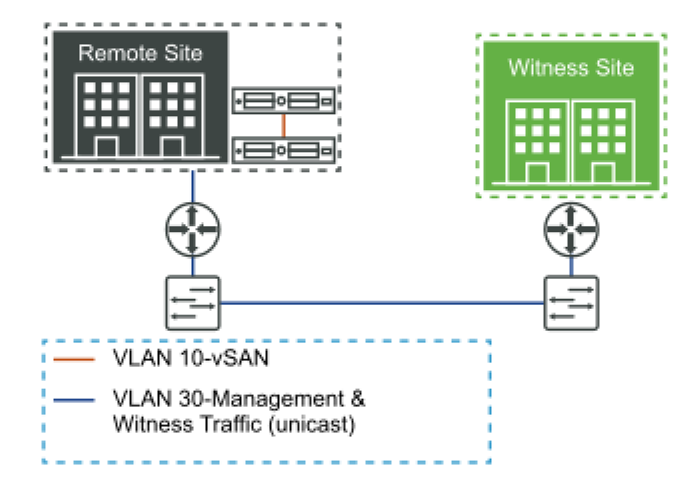
PIM no es necesario, ya que el único tráfico enrutado es el tráfico testigo, que es de unidifusión.




## Implementaciones de dos nodos para vSAN 6.5 y versiones posteriores

vSAN 6.5 y versiones posteriores admiten implementaciones de dos nodos.

Con vSAN 6.5 y versiones posteriores, esta implementación de vSAN de dos nodos es mucho más sencilla. vSAN 6.5 y las versiones posteriores permiten que los dos hosts del sitio de datos estén conectados directamente.

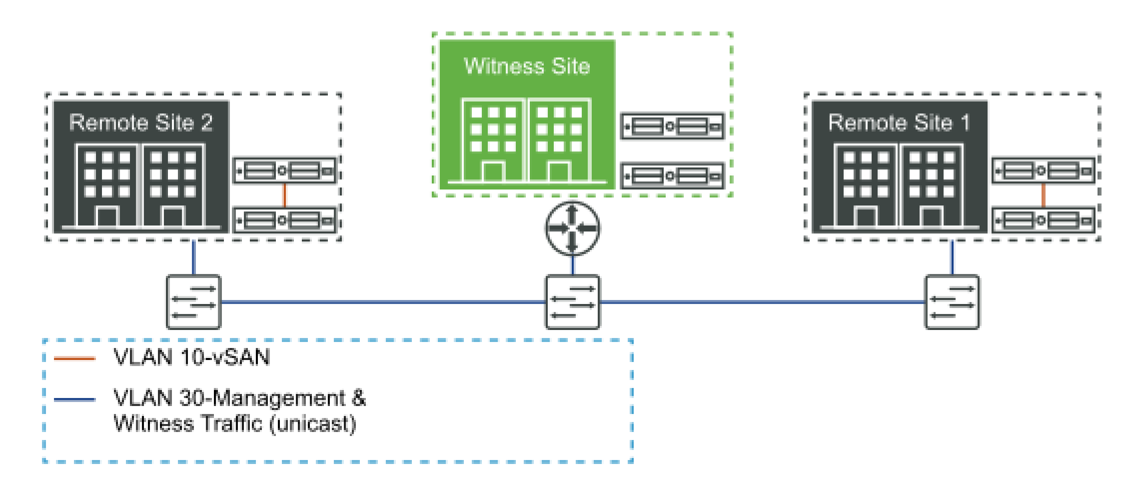



Para habilitar esta funcionalidad, el tráfico testigo se separa por completo del tráfico de datos de vSAN. El tráfico de datos de vSAN puede fluir entre los dos nodos de la conexión directa, mientras que el tráfico testigo se puede enrutar al sitio testigo a través de la red de administración.

El dispositivo testigo puede estar ubicado de forma remota de la sucursal. Por ejemplo, es posible que el testigo se vuelva a ejecutar en el centro de datos principal, junto con la infraestructura de administración (vCenter Server, vROps, Log Insight, etc.). Otra ubicación remota de la sucursal en la que puede residir el testigo es vCloud Air.

En esta configuración, no hay ningún conmutador en el sitio remoto. Como resultado, no es necesario configurar la compatibilidad con el tráfico de multidifusión en las redes consecutivas de vSAN. No es necesario tener en cuenta la multidifusión en la red de administración, ya que el tráfico testigo es de unidifusión.

vSAN 6.6 y versiones posteriores utilizan toda la desdifusión, por lo que no hay ninguna consideración de multidifusión. También se admiten varias implementaciones de dos nodos ROBO, siempre que cada una tenga su propio testigo único.




## Consideraciones comunes para las implementaciones de vSAN de dos nodos

Las implementaciones de vSAN de dos nodos son compatibles con otras topologías. En esta sección se describen las configuraciones comunes.

Para obtener más información sobre las configuraciones de dos nodos y las consideraciones de implementación detalladas fuera de la red, consulte la documentación principal de vSAN.

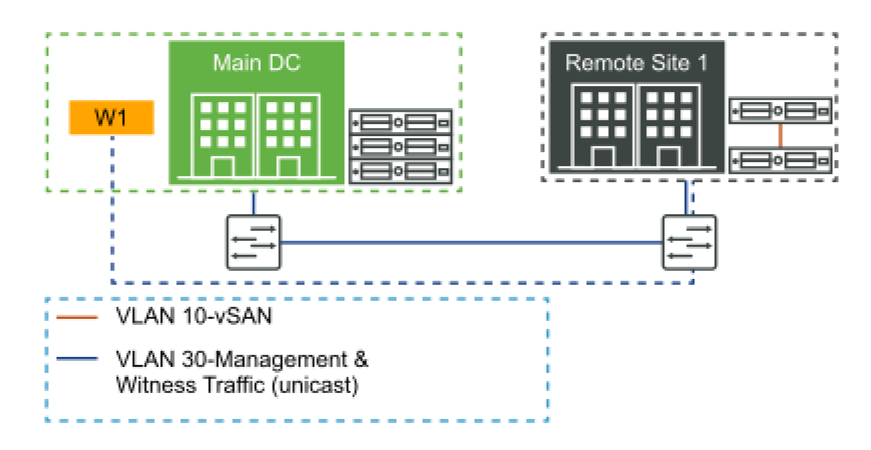
## Ejecutar el testigo en otro clúster de dos nodos

vSAN no admite la ejecución del testigo en otro clúster de dos nodos.

## Testigo ejecutado en otra implementación de vSAN estándar

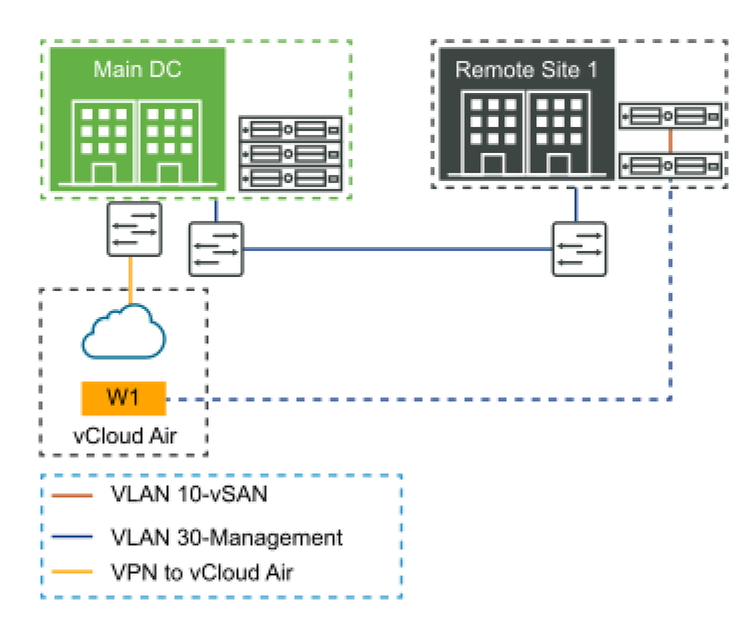
vSAN admite testigos que se ejecutan en otra implementación de vSAN estándar.

Esta configuración es admitida. Cualquier error en la implementación de vSAN de dos nodos en el sitio remoto no afecta a la disponibilidad del entorno de vSAN estándar en el centro de datos principal.




## Testigo ejecutado en vCloud Air

vSAN permite ejecutar un testigo en vCloud Air.




# Configuración de la red desde los sitios de datos al host testigo

Las interfaces de host de los sitios de datos se comunican con el host testigo a través de la red de vSAN. Existen diferentes opciones de configuración disponibles.

En este tema se analiza cómo implementar estas configuraciones. Soluciona el modo en que las interfaces de los hosts de los sitios de datos, que se comunican entre sí a través de la red de vSAN, se comunican con el host testigo.

## Opción 1: Host testigo ESXi físico conectado a través de capa 3 con rutas estáticas

Los sitios de datos se pueden conectar a través de una red de capa 2 ampliada. Use esto también para la red de administración de los sitios de datos, la red de vSAN, la red de vMotion y la red de máquinas virtuales.

El enrutador de red física de esta infraestructura de red no transfiere automáticamente el tráfico desde los hosts de los sitios de datos (sitio 1 y sitio 2) al host en el sitio testigo (sitio 3). Para poder configurar el clúster ampliado vSAN correctamente, todos sus hosts deben poder comunicarse. Es posible implementar un clúster ampliado en este entorno.

La solución es utilizar *rutas estáticas* configuradas en los hosts ESXi, de modo que el tráfico de vSAN procedente del sitio 1 y el sitio 2 llegue al host testigo en el sitio 3. En el caso de los hosts ESXi de los sitios de datos, agregue una ruta estática a la interfaz de vSAN, que redirige el tráfico al host testigo del sitio 3 a través de una puerta de enlace especificada para esa red. En el caso del host testigo, se debe agregar una ruta estática a la interfaz de vSAN, que redireccionará el tráfico de vSAN destinado a los hosts en los sitios de datos. Utilice el siguiente comando para agregar una ruta estática en cada host ESXi del clúster ampliado: **`esxcli network ip route ipv4 add -g`** *<puerta de enlace>* **`-n`** *<red>*

---

**Nota** vCenter Server debe ser capaz de administrar los hosts ESXi en los sitios de datos y en el sitio testigo. Siempre que haya conectividad directa desde el host testigo a vCenter Server, no tendrá que preocuparse de la red de administración.

---

No es necesario configurar una red de vMotion o de máquinas virtuales ni agregar rutas estáticas para estas redes en un clúster ampliado de vSAN. Las máquinas virtuales nunca se migran ni se implementan en el host testigo vSAN. Su finalidad es mantener solo los objetos testigo y no necesita ninguna de estas redes para esta tarea.

## Opción 2: Dispositivo testigo ESXi virtual conectado a través de la capa 3 con rutas estáticas

Dado que el host testigo es una máquina virtual que se implementa en un host ESXi físico que no forma parte del clúster de vSAN, dicho host ESXi físico debe tener al menos una red de máquinas virtuales configurada previamente. Esta red de máquinas virtuales debe poder comunicarse tanto con la red de administración como con la red de vSAN compartida por los hosts ESXi en los sitios de datos.

---

**Nota** El host testigo no necesita ser un host dedicado. Se puede utilizar para muchas otras cargas de trabajo de máquinas virtuales, mientras que aloja el testigo al mismo tiempo. Muchas organizaciones eligen su infraestructura de administración para alojar el dispositivo testigo en los hosts o el clúster donde se ejecutan vCenter Server, vRealize Operations o Log Insight.

---

Una opción alternativa es tener dos redes de máquinas virtuales configuradas previamente en el host ESXi físico subyacente, una para la red de administración y otra para la red de vSAN. Cuando el host testigo ESXi virtual se implementa en este host ESXi físico, la red debe estar conectada y configurada según corresponda.

Una vez que haya implementado el host testigo ESXi virtual, configure la ruta estática. Supongamos que los sitios de datos están conectados a través de una red de capa 2 ampliada. Use esto también para la red de administración de los sitios de datos, la red de vSAN, la red de vMotion y la red de máquinas virtuales. El tráfico de vSAN no se enruta desde los hosts de los sitios de datos (sitio 1 y sitio 2) al host del sitio testigo (sitio 3) a través de la puerta de enlace predeterminada. Para configurar el clúster ampliado de vSAN correctamente, todos los hosts del clúster requieren rutas estáticas, de modo que el tráfico de vSAN desde el sitio 1 y el sitio 2 llegue al host testigo en el sitio 3. Use el comando **`esxcli network ip route`** para agregar una ruta estática en cada host ESXi.

# Implementaciones para casos límite

Es posible implementar vSAN en configuraciones inusuales o casos límite.

Estas topologías inusuales requieren consideraciones especiales.

## Tres ubicaciones, sin clúster ampliado, hosts testigo distribuidos

Puede implementar vSAN en varias salas, edificios o sitios en lugar de implementar una configuración de clúster ampliado.

Esta configuración es admitida. El único requisito es que la latencia entre los sitios debe estar en el mismo nivel que la latencia esperada para una implementación de vSAN normal en el mismo centro de datos. La latencia debe ser **<1ms** entre todos los hosts. Si es mayor que este valor, use un clúster ampliado que tolere una latencia de 5 ms. Con vSAN 6.5 o versiones anteriores, deben tenerse en cuenta consideraciones adicionales para la multidifusión.

Para obtener los mejores resultados, mantenga una configuración uniforme en todos los sitios de una topología de este tipo. Para mantener la disponibilidad de las máquinas virtuales, configure dominios de errores, donde los hosts de cada sala, edificio o sitio se colocan en el mismo dominio de errores. Evite la partición asimétrica del clúster, donde el host A no puede comunicarse con el host B, pero el host B sí puede comunicarse con el host A.

## Dos nodos implementados como un clúster ampliado 1+1+W

Puede implementar una configuración de dos nodos como una configuración de clúster ampliado, colocando cada host en diferentes salas, edificios o sitios.

Se produce un error de licencia al intentar aumentar el número de hosts en cada sitio. Para cualquier clúster que tenga más de dos hosts y que utilice la función host/dispositivo testigo dedicado (N+N+Testigo, donde N>1), la configuración se considera un clúster ampliado de vSAN.

# Solución de errores de las redes vSAN

13

vSAN permite examinar y solucionar distintos tipos de problemas que surgen de una red de vSAN mal configurada.

Las operaciones de vSAN dependen de la configuración, la fiabilidad y el rendimiento de la red. Muchas solicitudes de soporte técnico provienen de una configuración de red incorrecta o de que la red no funciona según lo esperado.

Use el servicio de estado de vSAN para resolver problemas de red. Las comprobaciones del estado de la red pueden dirigirle a un artículo de la base de conocimientos adecuado, según los resultados de la comprobación de estado. El artículo de la base de conocimientos le proporcionará instrucciones para solucionar el problema de red.

## Comprobaciones de estado de red

El servicio de estado incluye una categoría para las comprobaciones de estado de redes.

Cada comprobación de estado tiene un enlace **AskVMware**. Si se produce un error en una comprobación de estado, haga clic en **AskVMware** y lea el artículo de la base de conocimientos de VMware asociado para obtener más información y las instrucciones para solucionar el problema.

Las siguientes comprobaciones de estado de redes ofrecen información útil sobre el entorno de vSAN.

- vSAN**: Comprobación básica de conectividad (unidifusión)**. Esta comprobación verifica que existe conectividad IP entre todos los hosts ESXi del clúster de vSAN haciendo ping a cada host ESXi de la red de vSAN desde cada host ESXi.
- **vMotion: Comprobación básica de conectividad (unidifusión)**. Esta comprobación verifica que existe conectividad IP entre todos los hosts ESXi del clúster de vSAN que tengan vMotion configurado. Cada host ESXi de la red de vMotion hace ping a los demás hosts ESXi.
- **Todos los hosts tienen una vmknic de vSAN configurada**. Esta comprobación garantiza que cada host ESXi del clúster de vSAN tenga una NIC de VMkernel configurada para el tráfico de vSAN.
- Todos los hosts tienen configuración de multidifusión coincidente. Esta comprobación garantiza que cada host tenga una dirección de multidifusión configurada correctamente.

- **Todos los hosts tienen subredes coincidentes**. Esta comprobación verifica que todos los hosts ESXi de un clúster de vSAN se hayan configurado para que todas las NIC VMkernel de vSAN estén en la misma subred IP.
- **Hosts desconectados de VC**. Esta comprobación verifica que vCenter Server tiene una conexión activa con todos los hosts ESXi en el clúster de vSAN.
- **Hosts con problemas de conectividad**. Esta comprobación hace referencia a situaciones en las que las listas de vCenter Server muestran el host como conectado, pero las llamadas de la API desde vCenter al host están fallando. Puede resaltar los problemas de conectividad entre un host y vCenter Server.
- **Latencia de red**. Esta comprobación verifica la latencia de red de los hosts vSAN. Si el umbral supera los 100 ms, se mostrará una advertencia. Si el umbral de latencia supera 200 ms, se producirá un error.
- **vMotion: prueba de MTU (ping con tamaño de paquete grande)**. Esta comprobación complementa la comprobación de conectividad de ping de vMotion básica. El tamaño máximo de la unidad de transmisión aumenta para mejorar el rendimiento de la red. Es posible que las MTU configuradas de forma incorrecta no aparezcan como un problema de configuración de red, pero pueden causar problemas de rendimiento.
- **Partición de clúster de vSAN**. Esta comprobación de estado examina el clúster para ver cuántas particiones existen. Muestra un error si hay más de una partición en el clúster de vSAN.
- **Evaluación de multidifusión basada en otras comprobaciones**. Esta comprobación de estado agrega datos de todas las comprobaciones de estado de la red. Si se produce un error en esta comprobación, indica que es probable que la multidifusión sea la causa principal de una partición de red.

## Comandos para comprobar la red

Cuando se haya configurado la red vSAN, utilice estos comandos para comprobar su estado. Puede comprobar qué adaptador de VMkernel (vmknic) se utiliza para vSAN y qué atributos contiene.

Utilice los comandos ESXCLI y RVC para comprobar que la red funciona perfectamente y solucionar cualquier problema de red con vSAN.

Puede comprobar que los vmknic utilizados para la red de vSAN estén configurados de manera uniforme en todos los hosts, comprobar que la multidifusión sea funcional y que los hosts que participan en el clúster de vSAN pueden comunicarse correctamente entre sí.

## esxcli vsan network list

Este comando permite identificar la interfaz de VMkernel que utiliza la red de vSAN.

El siguiente resultado muestra que la red vSAN está utilizando vmk2. Este comando sigue funcionando aunque vSAN se haya deshabilitado en el clúster y los hosts ya no participen en vSAN.

Es importante comprobar también la multidifusión del grupo de agentes y la multidifusión del grupo maestro.

```
[root@esxi-dell-m:~] esxcli vsan network list
Interface
   VmkNic Name: vmk1
   IP Protocol: IP
   Interface UUID: 32efc758-9ca0-57b9-c7e3-246e962c24d0
   Agent Group Multicast Address: 224.2.3.4
   Agent Group IPv6 Multicast Address: ff19::2:3:4
   Agent Group Multicast Port: 23451
   Master Group Multicast Address: 224.1.2.3
   Master Group IPv6 Multicast Address: ff19::1:2:3
   Master Group Multicast Port: 12345
   Host Unicast Channel Bound Port: 12321
   Multicast TTL: 5
   Traffic Type: vsan
```

Esto proporciona información útil, como la interfaz de VMkernel que se utiliza para el tráfico de vSAN. En este caso, es **vmk1**. Sin embargo, también se muestran las direcciones de multidifusión. Es posible que esta información se muestre incluso cuando el clúster se ejecuta en modo de unidifusión. Existe el puerto y la dirección de multidifusión del grupo. El puerto 23451 se utiliza para el latido, enviado cada segundo por el principal, y es visible en los demás hosts del clúster. El puerto 12345 se utiliza para las actualizaciones de CMMDS entre el principal y la copia de seguridad.

# esxcli network ip interface list

Este comando permite verificar elementos como vSwitch o conmutadores distribuidos.

Utilice este comando para comprobar a qué vSwitch o conmutador distribuido está asociado y el tamaño de MTU, que puede resultar útil si se han configurado tramas gigantes en el entorno. En este caso, MTU tiene el valor predeterminado de 1500.

```
[root@esxi-dell-m:~] esxcli network ip interface list
vmk0
   Name: vmk0
   <<truncated>>
vmk1
   Name: vmk1
   MAC Address: 00:50:56:69:96:f0
   Enabled: true
   Portset: DvsPortset-0
   Portgroup: N/A
   Netstack Instance: defaultTcpipStack
   VDS Name: vDS
   VDS UUID: 50 1e 5b ad e3 b4 af 25-18 f3 1c 4c fa 98 3d bb
```

```
    VDS Port: 16
    VDS Connection: 1123658315
    Opaque Network ID: N/A
    Opaque Network Type: N/A
    External ID: N/A
    MTU: 9000
    TSO MSS: 65535
    Port ID: 50331814
```

El tamaño de la unidad de transmisión máxima se muestra como 9000, por lo que este puerto de VMkernel se configura para las tramas gigantes, que requieren una MTU de aproximadamente 9000. VMware no realiza ninguna recomendación sobre el uso de tramas gigantes. Sin embargo, se admite el uso de tramas gigantes con vSAN.

## esxcli network ip interface ipv4 get –i vmk2

Este comando muestra información como la dirección IP y la máscara de red de la interfaz de VMkernel de vSAN.

Con esta información, un administrador ahora puede empezar a utilizar otros comandos disponibles en la línea de comandos para comprobar que la red vSAN funciona correctamente.

```
[root@esxi-dell-m:~] esxcli network ip interface ipv4 get -i vmk1
Name  IPv4 Address  IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway  DHCP DNS
----  ------------  -------------  --------------  ------------  -------  --------
vmk1  172.40.0.9   255.255.255.0   172.40.0.255   STATIC         0.0.0.0 false
```

## vmkping

El comando `vmkping` comprueba si los demás hosts ESXi de la red responden a sus solicitudes de ping.

```
~ # vmkping -I vmk2 172.32.0.3 -s 1472 -d
 PING 172.32.0.3 (172.32.0.3): 56 data bytes
 64 bytes from 172.32.0.3: icmp_seq=0 ttl=64 time=0.186 ms
 64 bytes from 172.32.0.3: icmp_seq=1 ttl=64 time=2.690 ms
 64 bytes from 172.32.0.3: icmp_seq=2 ttl=64 time=0.139 ms

 --- 172.32.0.3 ping statistics ---
 3 packets transmitted, 3 packets received, 0% packet loss
 round-trip min/avg/max = 0.139/1.005/2.690 ms
```

Aunque no se verifica la funcionalidad de multidifusión, puede ayudar a identificar un host ESXi malintencionado que tenga problemas de red. También puede examinar los tiempos de respuesta para ver si hay latencia anormal en la red de vSAN.

Si se configuran tramas gigantes, este comando no encontrará ningún problema si el tamaño de la MTU de las tramas gigantes es incorrecto. De forma predeterminada, este comando utiliza un tamaño de MTU de 1500. Si es necesario comprobar si las tramas gigantes funcionan correctamente de extremo a extremo, use vmkping con una opción de tamaño de paquete (-s) mayor, como se indica a continuación:

```
~ # vmkping -I vmk2 172.32.0.3 -s 8972 -d
PING 172.32.0.3 (172.32.0.3): 8972 data bytes
9008 bytes from 172.32.0.3: icmp_seq=0 ttl=64 time=0.554 ms
9008 bytes from 172.32.0.3: icmp_seq=1 ttl=64 time=0.638 ms
9008 bytes from 172.32.0.3: icmp_seq=2 ttl=64 time=0.533 ms

--- 172.32.0.3 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.533/0.575/0.638 ms
~ #
```

Puede agregar -d al comando vmkping para probar si los paquetes se pueden enviar sin fragmentación.

# esxcli network ip neighbor list

Este comando ayuda a comprobar si todos los hosts vSAN se encuentran en el mismo segmento de red.

En esta configuración, tenemos un clúster con cuatro hosts y este comando devuelve las entradas ARP (Protocolo de resolución de direcciones) de los otros tres hosts, incluidas sus direcciones IP y sus vmknic (vSAN está configurado para usar vmk1 en todos los hosts de este clúster).

```
[root@esxi-dell-m:~] esxcli network ip neighbor list -i vmk1
Neighbor     Mac Address        Vmknic   Expiry  State  Type
-----------  -----------------  ------  -------  -----  -------
172.40.0.12  00:50:56:61:ce:22  vmk1    164 sec         Unknown
172.40.0.10  00:50:56:67:1d:b2  vmk1    338 sec         Unknown
172.40.0.11  00:50:56:6c:fe:c5  vmk1    162 sec         Unknown
[root@esxi-dell-m:~]
```

# esxcli network diag ping

Este comando comprueba los duplicados en la red y los tiempos de ida y vuelta.

Para obtener más información sobre la conectividad de redes vSAN entre los distintos hosts, ESXCLI ofrece un comando de diagnóstico de red eficaz. A continuación se muestra un ejemplo de un resultado, en el que la interfaz de VMkernel se encuentra en vmk1 y la IP de red de vSAN remota de otro host de la red es 172.40.0.10

```
[root@esxi-dell-m:~] esxcli network diag ping -I vmk1 -H 172.40.0.10
   Trace:
         Received Bytes: 64
```

```
          Host: 172.40.0.10
          ICMP Seq: 0
          TTL: 64
          Round-trip Time: 1864 us
          Dup: false
          Detail:

          Received Bytes: 64
          Host: 172.40.0.10
          ICMP Seq: 1
          TTL: 64
          Round-trip Time: 1834 us
          Dup: false
          Detail:

          Received Bytes: 64
          Host: 172.40.0.10
          ICMP Seq: 2
          TTL: 64
          Round-trip Time: 1824 us
          Dup: false
          Detail:
    Summary:
          Host Addr: 172.40.0.10
          Transmitted: 3
          Recieved: 3
          Duplicated: 0
          Packet Lost: 0
          Round-trip Min: 1824 us
          Round-trip Avg: 1840 us
          Round-trip Max: 1864 us
[root@esxi-dell-m:~]
```

# vsan.lldpnetmap

Este comando de RVC muestra la información del puerto de vínculo superior.

Si hay conmutadores que no son de Cisco con el protocolo de detección de nivel de vínculo (LLDP) habilitado en el entorno, existe un comando de RVC para mostrar la siguiente información: vínculo superior <-> conmutador <-> puerto del conmutador. Para obtener más información sobre RVC, consulte la guía de comandos de RVC.

Esto le ayudará a determinar qué hosts están conectados a qué conmutadores cuando el clúster de vSAN abarca varios conmutadores. Puede ayudar a aislar un problema en un determinado conmutador cuando solo se ve afectado un subconjunto de los hosts del clúster.

```
> vsan.lldpnetmap 02013-08-15 19:34:18 -0700: This operation will take
30-60 seconds ...+---------------+---------------------------+| Host          | LLDP
info                 |+---------------+---------------------------+| 10.143.188.54 | w2r13-
vsan-x650-2: vmnic7 ||               | w2r13-vsan-x650-1: vmnic5 |+---------------
+---------------------------+
```

Esto solo está disponible con los conmutadores que admiten LLDP. Para configurarlo, inicie sesión en el conmutador y ejecute lo siguiente:

```
switch# config t
Switch(Config)# feature lldp
```

Para verificar que LLDP está habilitado:

```
switch(config)#do show running-config lldp
```

**Nota** LLDP funciona en modo de envío y recepción de forma predeterminada. Compruebe la configuración de las propiedades del vDS si no se detecta la información del conmutador físico. De forma predeterminada, el vDS se crea con el protocolo de detección configurado en CDP (Cisco Discovery Protocol). Para solucionar este error, establezca el protocolo de detección en LLDP y establezca la operación en **Ambos** en el vDS.

## Comprobar las comunicaciones de multidifusión

Las configuraciones de multidifusión pueden causar problemas en la implementación inicial de vSAN.

Una de las formas más sencillas de comprobar si la multidifusión funciona correctamente en el entorno de vSAN es mediante el comando `tcpdump-uw`. Este comando está disponible en la línea de comandos de los hosts ESXi.

El comando `tcpdump-uw` muestra si el principal está enviando correctamente paquetes de multidifusión (información de puerto e IP) y si los demás hosts del clúster los reciben.

En el nodo principal, este comando muestra los paquetes que se envían a la dirección de multidifusión. En los demás hosts, los mismos paquetes son visibles (desde el principal a la dirección de multidifusión). Si no están visibles, la multidifusión no funciona correctamente. Ejecute el comando `tcpdump-uw` que se muestra aquí en cualquier host del clúster y los latidos del principal estarán visibles. En este caso, el nodo principal se encuentra en la dirección IP 172.32.0.2. El uso de **-v** para nivel de detalle es opcional.

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast -v
tcpdump-uw: listening on vmk2, link-type EN10MB (Ethernet), capture size 96 bytes
11:04:21.800575 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 34917, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:04:22.252369 IP truncated-ip - 234 bytes missing! (tos 0x0, ttl 5, id 15011, offset 0,
flags [none], proto UDP (17), length 316)
    172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:04:22.262099 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 3359, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
11:04:22.324496 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 20914, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.5.60460 > 224.1.2.3.12345: UDP, length 200
11:04:22.800782 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 35010, offset 0,
```

```
flags [none], proto UDP (17), length 228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:04:23.252390 IP truncated-ip - 234 bytes missing! (tos 0x0, ttl 5, id 15083, offset 0,
flags [none], proto UDP (17), length 316)
    172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:04:23.262141 IP truncated-ip - 146 bytes missing! (tos 0x0, ttl 5, id 3442, offset 0,
flags [none], proto UDP (17), length 228)
    172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
```

Aunque esta solución puede parecer un poco confusa, basta con decir que el resultado que se muestra aquí indica que los cuatro hosts del clúster están recibiendo un latido del principal. Se debe ejecutar el comando **tcpdump-uw** en cada host para comprobar que todos están recibiendo el latido. Esto comprueba que el principal está enviando los latidos y que los demás hosts del clúster los están recibiendo, lo que indica que la multidifusión funciona.

Si algunos de los hosts de vSAN no reciben los latidos de un segundo del principal, el administrador de red debe comprobar la configuración de multidifusión de sus conmutadores.

Para evitar el molesto mensaje **truncated-ip – 146 bytes missing!**, utilice la opción **-s0** en el mismo comando para detener el truncado de paquetes:

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast -v -s0
tcpdump-uw: listening on vmk2, link-type EN10MB (Ethernet), capture size 65535 bytes
11:18:29.823622 IP (tos 0x0, ttl 5, id 56621, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
11:18:30.251078 IP (tos 0x0, ttl 5, id 52095, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.3.41220 > 224.2.3.4.23451: UDP, length 200
11:18:30.267177 IP (tos 0x0, ttl 5, id 8228, offset 0, flags [none], proto UDP (17), length
316)
    172.32.0.2.38170 > 224.2.3.4.23451: UDP, length 288
11:18:30.336480 IP (tos 0x0, ttl 5, id 28606, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.5.60460 > 224.1.2.3.12345: UDP, length 200
11:18:30.823669 IP (tos 0x0, ttl 5, id 56679, offset 0, flags [none], proto UDP (17), length
228)
    172.32.0.4.44824 > 224.1.2.3.12345: UDP, length 200
```

El comando **tcpdump** está relacionado con la pertenencia a IGMP (protocolo de administración de grupos de Internet). Los hosts (y los dispositivos de red) utilizan IGMP para establecer la pertenencia al grupo de multidifusión.

Cada host ESXi en el clúster de vSAN envía informes de pertenencia IGMP normales (Unirse).

El comando **tcpdump** muestra los informes de miembros de IGMP de un host:

```
[root@esxi-dell-m:~] tcpdump-uw -i vmk1 igmp
tcpdump-uw: verbose output suppressed, use -v or -vv for full protocol decode
listening on vmk1, link-type EN10MB (Ethernet), capture size 262144 bytes
15:49:23.134458 IP 172.40.0.9 > igmp.mcast.net: igmp v3 report, 1 group record(s)
15:50:22.994461 IP 172.40.0.9 > igmp.mcast.net: igmp v3 report, 1 group record(s)
```

El resultado muestra que los informes de IGMP v3 se están realizando, lo que indica que el host ESXi está actualizando su pertenencia de forma regular. Si un administrador de red tiene dudas sobre si los hosts ESXi de vSAN están realizando IGMP de forma correcta, ejecute este comando en cada host ESXi del clúster y use este seguimiento para comprobarlo.

Si tiene comunicaciones de multidifusión, use IGMP 3.

De hecho, el siguiente comando se puede utilizar para ver el tráfico de multidifusión e IGMP al mismo tiempo:

```
[root@esxi-hp-02:~] tcpdump-uw -i vmk2 multicast or igmp -v -s0
```

Un problema común es que el clúster de vSAN está configurado en varios conmutadores físicos y, mientras que la multidifusión se habilitó en un conmutador, no se habilitó en todos los conmutadores. En este caso, el clúster se crea con dos hosts ESXi en una partición y otro host ESXi (conectado al otro conmutador) no puede unirse a este clúster. En su lugar, crea su propio clúster de vSAN en otra partición. El comando `vsan.lldpnetmap` que vimos antes le ayudará a determinar la configuración de red y los hosts asociados a ese conmutador.

Mientras se crea un clúster de vSAN, hay indicadores que muestran que la multidifusión pueden ser un problema.

Supongamos que siguió la lista de comprobación de subred, VLAN y MTU, y cada host del clúster puede hacer `vmkping` en todos los hosts del clúster.

Si se produce un problema de multidifusión cuando se crea el clúster, un síntoma común es que cada host ESXi crea su propio clúster vSAN, con él mismo como principal. Si cada host tiene un identificador de partición de red único, este síntoma sugiere que no hay multidifusión entre cualquiera de los hosts.

Sin embargo, si un subconjunto de los hosts ESXi crea un clúster y otro subconjunto crea otro clúster, y cada uno tiene particiones únicas con su propio principal, su propia copia de seguridad e incluso sus propios hosts de agente, la multidifusión se habilita en el conmutador, pero no entre conexiones. vSAN muestra los hosts en el primer conmutador físico creando su propia partición del clúster, y los hosts del segundo conmutador físico creando también su propia partición del clúster, cada uno con su propio principal. Si puede verificar a qué conmutadores se conectan los hosts del clúster y si los hosts de un clúster están conectados al mismo conmutador, es probable que este sea el problema.

# Comprobar el rendimiento de las redes de vSAN

Asegúrese de que haya suficiente ancho de banda entre los hosts ESXi. Esta herramienta puede ayudarle a probar si la red de vSAN funciona de forma óptima.

Para comprobar el rendimiento de la red de vSAN, puede usar la herramienta `iperf` para medir la latencia y el ancho de banda de TCP máximos. Se encuentra en `/usr/lib/vmware/vsan/bin/iperf.copy`. Ejecútela con `--help` para ver las distintas opciones. Use esta herramienta para comprobar el ancho de banda y la latencia de la red entre los hosts ESXi que participan en un clúster de vSAN.

El artículo 2001003 de la base de conocimientos de VMware incluye información sobre la configuración y las pruebas.

Esto resulta especialmente útil cuando se realiza una puesta en servicio de un clúster de vSAN. La ejecución de las pruebas **iperf** en la red de vSAN cuando el clúster ya está en producción puede afectar al rendimiento de las máquinas virtuales que se ejecutan en el clúster.

# Comprobar los límites de red de vSAN

El comando **vsan.check.limits** permite comprobar que no se esté infringiendo ninguno de los umbrales de vSAN.

```
> ls
0 /
1 vcsa-04.rainpole.com/
> cd 1
/vcsa-04.rainpole.com> ls
0 Datacenter (datacenter)
/vcsa-04.rainpole.com> cd 0
/vcsa-04.rainpole.com/Datacenter> ls
0 storage/
1 computers [host]/
2 networks [network]/
3 datastores [datastore]/
4 vms [vm]/
/vcsa-04.rainpole.com/Datacenter> cd 1
/vcsa-04.rainpole.com/Datacenter/computers> ls
0 Cluster (cluster): cpu 155 GHz, memory 400 GB
1 esxi-dell-e.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
2 esxi-dell-f.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
3 esxi-dell-g.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
4 esxi-dell-h.rainpole.com (standalone): cpu 38 GHz, memory 123 GB
/vcsa-04.rainpole.com/Datacenter/computers> vsan.check_limits 0
2017-03-14 16:09:32 +0000: Querying limit stats from all hosts ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-m.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-n.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-o.rainpole.com (may take a
moment) ...
2017-03-14 16:09:34 +0000: Fetching vSAN disk info from esxi-dell-p.rainpole.com (may take a
moment) ...
2017-03-14 16:09:39 +0000: Done fetching vSAN disk infos
+--------------------------+--------------------
+-----------------------------------------------------------------+
| Host                     | RDT
| Disks                                                           |
+--------------------------+--------------------
+-----------------------------------------------------------------+
| esxi-dell-m.rainpole.com |
Assocs: 1309/45000 | Components: 485/9000                                            |
|                          | Sockets:
89/10000  | naa.500a075113019b33: 0% Components: 0/0                         |
```

```
|                          | Clients:
136       | naa.500a075113019b37: 40% Components: 81/47661                  |
|                          | Owners:
138        | t10.ATA_____Micron_P420m2DMTFDGAR1T4MAX_____ 0% Components: 0/0 |
|                          |                     |
naa.500a075113019b41: 37% Components: 80/47661                |
|                          |                     |
naa.500a07511301a1eb: 38% Components: 81/47661                |
|                          |                     |
naa.500a075113019b39: 39% Components: 79/47661                |
|                          |                     |
naa.500a07511301a1ec: 41% Components: 79/47661                |
<<truncated>>
```

Desde el punto de vista de la red, lo importante son las asociaciones de RDT y el número de sockets. Hay 45.000 asociaciones por host en vSAN 6.0 y versiones posteriores. Se utiliza una asociación de RDT para supervisar el estado de la red de igual a igual en vSAN. El tamaño de vSAN se ajusta para que nunca se ejecute fuera de las asociaciones de RDT. vSAN también limita cuántos sockets TCP pueden usarse y se ajusta su tamaño para que nunca se agote su asignación de sockets TCP. Hay un límite de 10.000 sockets por host.

Un **cliente** vSAN representa el acceso del objeto en el clúster de vSAN. El cliente suele representar una máquina virtual que se ejecuta en un host. Es posible que el cliente y el objeto no estén en el mismo host. No hay ningún límite definido, pero esta métrica se muestra para ayudar a comprender el modo en que los clientes equilibran los hosts.

Solo hay un **propietario** de vSAN para cada objeto de vSAN, que normalmente se encuentra en la misma ubicación que el cliente de vSAN que accede a este objeto. Los propietarios de vSAN coordinan todo el acceso al objeto de vSAN e implementan funciones, como la creación de reflejos y la fragmentación. No hay ningún límite definido, pero esta métrica se muestra una vez más para ayudar a comprender el modo en que los propietarios equilibran los hosts.

# Usar la multidifusión en la red de vSAN

14

La multidifusión es una técnica de comunicación de red que envía paquetes de información a un grupo de destinos a través de una red IP.

Las versiones anteriores a vSAN 6.6 admiten la multidifusión IP y usaban la comunicación de multidifusión IP como protocolo de detección para identificar los nodos que intentan unirse a un clúster de vSAN. Las versiones anteriores a vSAN 6.6 dependen de la comunicación de multidifusión IP al unir y abandonar los grupos de clústeres y durante otras operaciones de comunicación dentro del clúster. Asegúrese de habilitar y configurar la multidifusión IP en los segmentos de red IP para transportar el servicio de tráfico de vSAN.

Una dirección de multidifusión IP se denomina grupo de multidifusión (MG). La multidifusión IP envía paquetes de origen a varios destinatarios como una transmisión de grupo. La multidifusión IP se basa en los protocolos de comunicación que los hosts, los clientes y los dispositivos de red utilizan para participar en las comunicaciones basadas en multidifusión. Los protocolos de comunicación, como el protocolo de administración de grupos de Internet (IGMP) y la multidifusión independiente de protocolo (PIM), son los componentes y las dependencias principales para el uso de las comunicaciones de multidifusión IP.

Al crear un clúster de vSAN, se asigna una dirección de multidifusión predeterminada a cada clúster de vSAN. El servicio de tráfico de vSAN asigna automáticamente la configuración de dirección de multidifusión predeterminada a cada host. Esta dirección de multidifusión envía tramas a un grupo de multidifusión y un agente de grupo de multidifusión predeterminados.

Cuando varios clústeres de vSAN residen en la misma red de capa 2, VMware recomienda cambiar la dirección de multidifusión predeterminada dentro de los clústeres de vSAN adicionales. Esto evita que varios clústeres reciban todas las transmisiones de multidifusión. Consulte el artículo 2075451 de la base de conocimientos de VMware para obtener más información sobre cómo cambiar la dirección multidifusión predeterminada de vSAN.

Este capítulo incluye los siguientes temas:

## Protocolo de administración de grupos de Internet

Puede utilizar el protocolo de administración de grupos de Internet (IGMP) para agregar receptores a la pertenencia a grupos de multidifusión IP dentro de los dominios de capa 2.

IGMP permite que los receptores envíen solicitudes a los grupos de multidifusión a los que desean unirse. Convertirse en miembro de un grupo de multidifusión permite a los enrutadores reenviar al puerto del conmutador el tráfico de los grupos de multidifusión en el segmento de capa 3 donde el receptor está conectado.

Puede usar la intromisión de IGMP para limitar los puertos del conmutador físico que participan en el grupo de multidifusión a solo vínculos superiores de puertos de VMkernel de vSAN. La intromisión de IGMP está configurada con un solicitante de intromisión de IGMP. La necesidad de configurar un solicitante de intromisión de IGMP para admitir la intromisión de IGMP varía según el proveedor del conmutador. Consulte al proveedor del conmutador específico para obtener la configuración de intromisión de IGMP.

vSAN es compatible con IGMP versión 2 e IGMP versión 3. Cuando se realiza la implementación de vSAN en varios segmentos de red de capa 3, se puede configurar un dispositivo compatible con la capa 3, como un enrutador o un conmutador con conexión y acceso a los mismos segmentos de red de capa 3.

Todos los puertos VMkernel de la red de vSAN se suscriben a un grupo de multidifusión mediante IGMP para evitar el desbordamiento de multidifusión en todos los puertos de red.

**Nota** Puede deshabilitar la intromisión de IGMP si vSAN se encuentra en una VLAN no enrutada o troncal que pueda extenderse a los puertos de vSAN de todos los hosts del clúster.

## Multidifusión independiente de protocolo

La multidifusión independiente de protocolo (PIM) consta de protocolos de enrutamiento de multidifusión de capa 3.

Proporciona diferentes técnicas de comunicación para el tráfico de multidifusión IP a los receptores de acceso que se encuentran en segmentos de capa 3 diferentes de los orígenes de los grupos de multidifusión. En versiones anteriores del clúster de vSAN 6.6, debe utilizar PIM para permitir que el tráfico de multidifusión fluya a través de diferentes subredes. Consulte a su proveedor de red para obtener la implementación de PIM.

# Consideraciones de redes para iSCSI en vSAN

15

El servicio del destino iSCSI de vSAN permite que los hosts y las cargas de trabajo físicas que se encuentren fuera del clúster de vSAN accedan al almacén de datos de vSAN. Esta característica permite que un iniciador iSCSI en un host remoto transporte datos a nivel de bloque a un destino iSCSI en un dispositivo de almacenamiento del clúster de vSAN.

Los destinos iSCSI en vSAN se administran mediante la administración basada en directivas de almacenamiento (SPBM), similar a otros objetos de vSAN. Esto permite ahorrar espacio y proporciona seguridad para los LUN de iSCSI a través de la desduplicación y compresión y el cifrado.. Para mejorar la seguridad, el servicio del destino iSCSI de vSAN usa el protocolo de autenticación por desafío mutuo (CHAP) y la autenticación de CHAP mutua.

vSAN identifica cada destino iSCSI con un nombre calificado de iSCSI (IQN) único. El destino iSCSI se presenta a un iniciador iSCSI remoto mediante el IQN, de modo que el iniciador puede acceder al LUN del destino. El servicio del destino iSCSI de vSAN permite crear grupos de iniciadores iSCSI. El grupo de iniciadores iSCSI solo permitirá el acceso de aquellos iniciadores que sean miembros del grupo.

Este capítulo incluye los siguientes temas:



## Características de la red iSCSI de vSAN

Estas son las características de las redes iSCSI de vSAN:

- Enrutamiento iSCSI: los iniciadores iSCSI pueden establecer conexiones enrutadas a destinos iSCSI de vSAN a través de una red de capa 3.
- IPv4 y IPv6: la red iSCSI de vSAN admite tanto IPv4 como IPv6.
- Seguridad IP: IPSec en la red iSCSI de vSAN proporciona mayor seguridad.

  **Nota** Los hosts ESXi admiten IPsec solo con IPv6.

- Tramas gigantes: las tramas gigantes son compatibles con la red iSCSI de vSAN.
- Formación de equipos de NIC: todas las configuraciones de formación de equipos de NIC son compatibles con la red iSCSI de vSAN.

- MCS (varias conexiones por sesión): la implementación iSCSI de vSAN no es compatible con MCS.

# Migrar de un vSwitch estándar a un vSwitch distribuido

16

Puede migrar de un conmutador estándar de vSphere a vSphere Distributed Switch y utilizar Network I/O Control. Esto le permitirá priorizar la QoS (calidad de servicio) en el tráfico de vSAN.

**Advertencia** Es mejor tener acceso a los hosts ESXi, aunque es posible que no lo necesite. Si algo sale mal, podrá acceder a la consola de los hosts ESXi.

Tome nota de la configuración del vSwitch original. En particular, tenga en cuenta la configuración de equilibrio de carga y de formación de equipos de NIC en el origen. Asegúrese de que la configuración de destino coincide con la de origen.

## Crear un conmutador distribuido

Cree el vSwitch distribuido y asígnele un nombre.

1 En la vista Hosts y clústeres de vSphere Client, haga clic con el botón derecho en un centro de datos y seleccione el menú **Nuevo Distributed Switch**.

2 Introduzca un nombre.

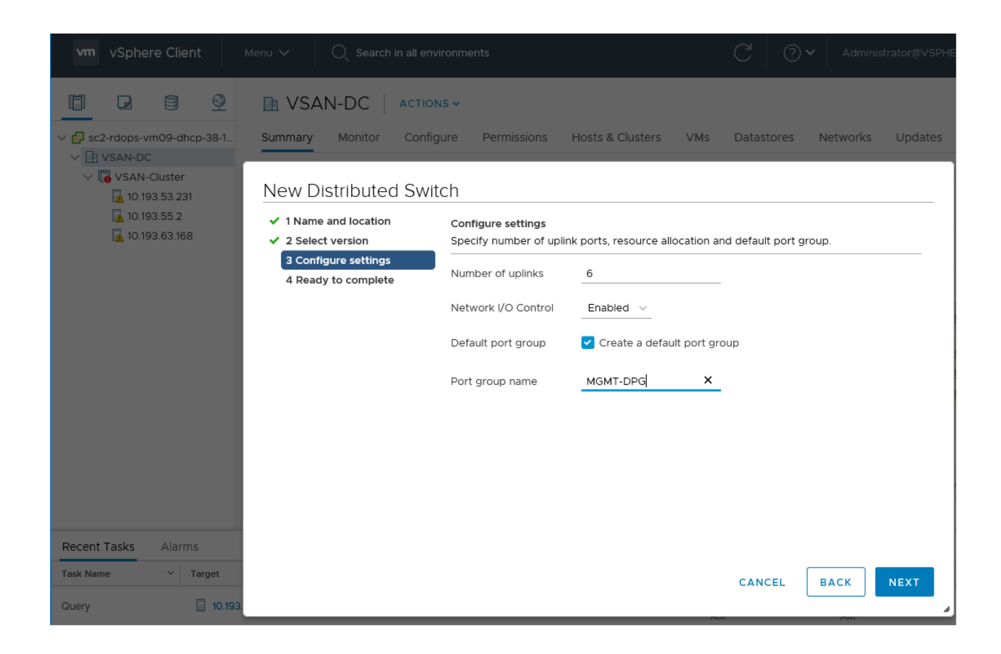
3 Seleccione la versión de vSphere Distributed Switch. En este ejemplo, se utiliza la versión 6.6.0 para la migración.

4 Agregue la configuración. Determine cuántos vínculos superiores está utilizando actualmente para las redes. En este ejemplo se usan seis: administración, vMotion, máquinas virtuales y tres para vSAN (una configuración LAG). Introduzca 6 para el número de vínculos superiores. Es posible que el entorno sea diferente, pero podrá editarlo más adelante.

   Puede crear un grupo de puertos predeterminado en este punto, pero se necesitan grupos de puertos adicionales.

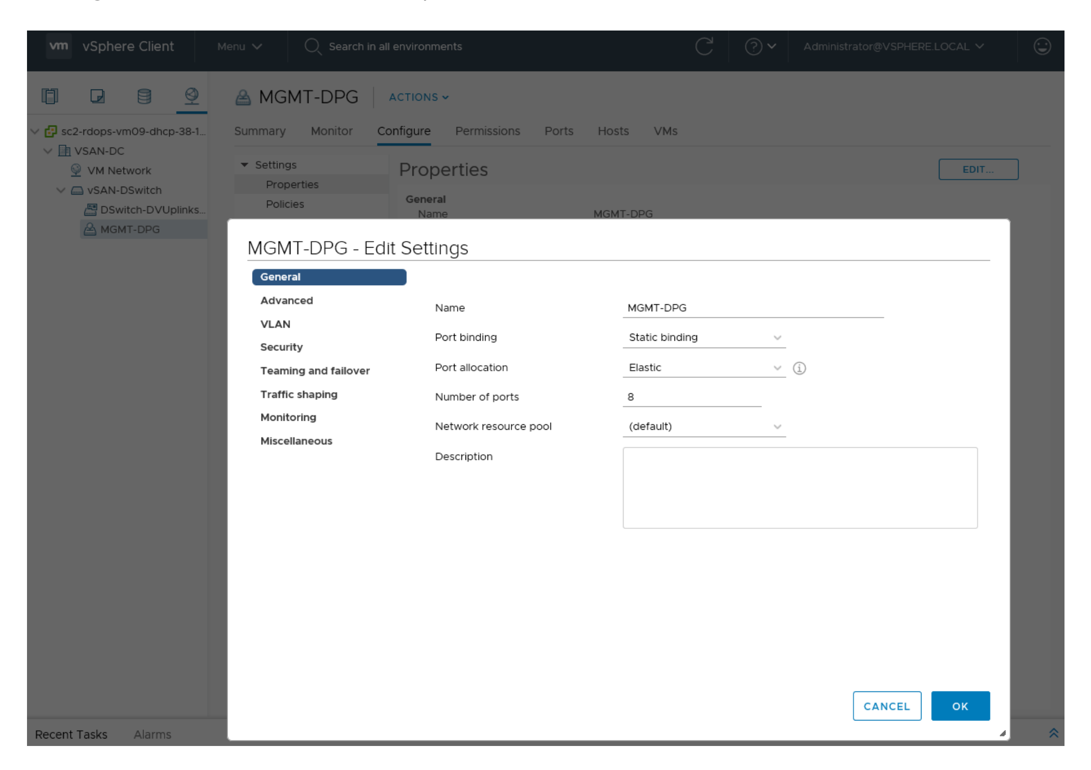
5 Finalice la configuración del vSwitch distribuido.

El siguiente paso consiste en configurar y crear los grupos de puertos adicionales.




# Crear grupos de puertos

Se creó un solo grupo de puertos predeterminado para la red de administración. Edite este grupo de puertos para asegurarse de que tiene todas las características del grupo de puertos de administración en el vSwitch estándar, como la formación de equipos de NIC y VLAN, y la configuración de conmutación por error.



Configure el grupo de puertos de administración.

1 En la vista Redes de vSphere Client, seleccione el grupo de puertos distribuidos y haga clic en **Editar**.

2 Para algunos grupos de puertos, debe cambiar la VLAN. Dado que la VLAN 51 es la VLAN de administración, etiquete el grupo de puertos distribuidos según corresponda.

3 Haga clic en **Aceptar**.

Cree grupos de puertos distribuidos para vMotion, redes de máquinas virtuales y redes de vSAN.

1 Haga clic con el botón derecho en el vSphere Distributed Switch y seleccione el menú **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

2 En este ejemplo, cree un grupo de puertos para la red de vMotion.

Cree todos los grupos de puertos distribuidos en el vSwitch distribuido. A continuación, migre los vínculos superiores, las redes de VMkernel y las redes de máquinas virtuales a los grupos de puertos distribuidos asociados y al vSwitch distribuido.

**Advertencia** Migre los vínculos superiores y las redes con mucho cuidado paso a paso.

# Migrar la red de administración

Migre la red de administración (vmk0) y su vínculo superior asociado (vmnic0) desde el vSwitch estándar al vSwitch distribuido (vDS).

1 Agregue hosts al vDS.

   a Haga clic con el botón derecho en el vDS y seleccione el menú **Agregar y administrar hosts**.

   b Agregue hosts al vDS. Haga clic en el icono Agregar verde (+) y agregue todos los hosts del clúster.

2 Configure los adaptadores físicos y los adaptadores de VMkernel.

   a Haga clic en **Administrar adaptadores físicos** para migrar los adaptadores físicos y los adaptadores VMkernel, vmnic0 y vmk0 al vDS.

   b Seleccione un vínculo superior adecuado en el vDS para el adaptador físico vmnic0. Para este ejemplo, utilice Uplink1. Se seleccionará el adaptador físico y se elegirá un vínculo superior.

3 Migre la red de administración en vmk0 desde el vSwitch estándar al vSwitch distribuido. Realice estos pasos en cada host.

   a Seleccione vmk0 y haga clic en **Asignar grupo de puertos**.

   b Asigne el grupo de puertos distribuidos creado anteriormente para la red de administración.

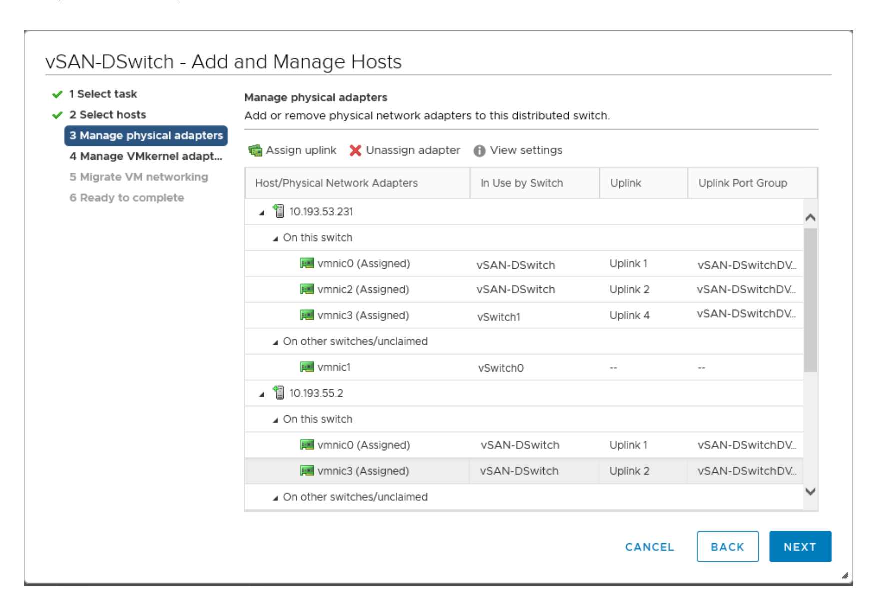
4 Finalice la configuración.

a Revise los cambios para asegurarse de que va a agregar cuatro hosts, cuatro vínculos superiores (vmnic0 desde cada host) y cuatro adaptadores de VMkernel (vmk0 desde cada host).

b Haga clic en **Finalizar**.

Al examinar la configuración de redes de cada host, revise la configuración del conmutador con un vínculo superior (vmnic0) y el puerto de administración de vmk0 en cada host.

Repita este proceso en las otras redes.




## Migrar vMotion

Para migrar la red de vMotion, siga los mismos pasos utilizados para la red de administración.

Antes de comenzar, asegúrese de que el grupo de puertos distribuidos para la red de vMotion tenga los mismos atributos que el grupo de puertos en el vSwitch estándar. A continuación, migre el vínculo superior utilizado para vMotion (vmnic1) con el adaptador de VMkernel (vmk1).

## Migrar red de vSAN

Si tiene un solo vínculo superior para la red de vSAN, utilice el mismo proceso que antes. Sin embargo, si utiliza más de un vínculo superior, deberá seguir pasos adicionales.

Si la red de vSAN utiliza la adición de enlaces (LACP) o se encuentra en una VLAN diferente a las otras redes de VMkernel, coloque algunos de los vínculos superiores en un estado Sin utilizar para ciertos adaptadores de VMkernel.

Por ejemplo, el adaptador de VMkernel vmk2 se utiliza para vSAN. Sin embargo, los vínculos superiores vmnic3, 4 y 5 se utilizan para vSAN y se encuentran en una configuración de LACP. Por lo tanto, para vmk2, los demás vmnics (0, 1 y 2) deben ponerse en un estado Sin utilizar. De forma similar, para el adaptador de administración (vmk0) y el adaptador de vMotion (vmk0), ponga los vínculos superiores/vmnics de vSAN en un estado Sin utilizar.

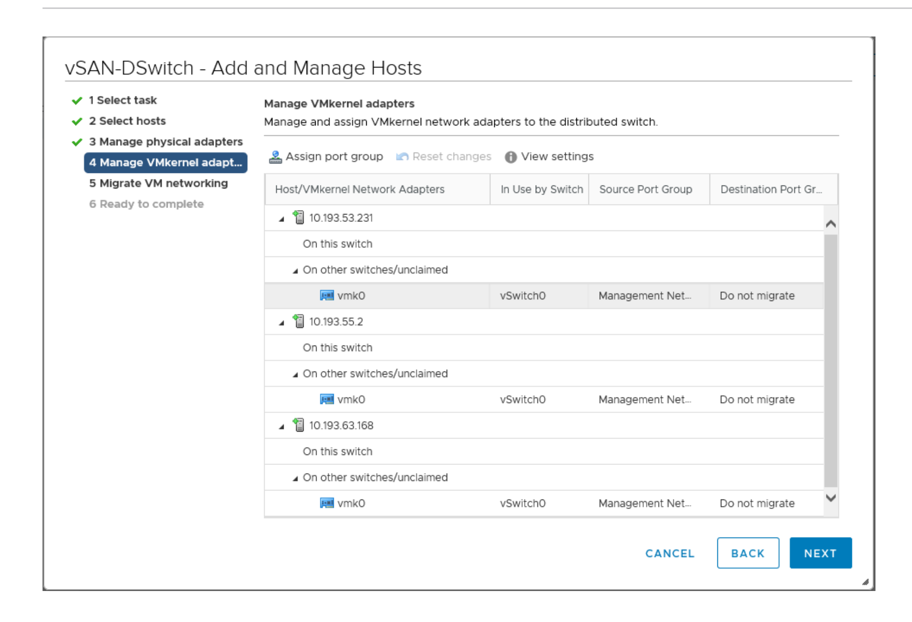
Modifique la configuración del grupo de puertos distribuidos y cambie la directiva de ruta y la configuración de conmutación por error. En la página **Administrar adaptador de red físico**, siga los pasos para varios adaptadores.

Asigne el adaptador de VMkernel vSAN (vmk2) al grupo de puertos distribuidos para vSAN.

---

**Nota** Si solo va a migrar los vínculos superiores de la red de vSAN, es posible que no pueda cambiar la configuración del grupo de puertos distribuidos hasta después de la migración. Durante este tiempo, es posible que vSAN tenga problemas de comunicación. Después de la migración, vaya a la configuración del grupo de puertos distribuidos y realice cualquier cambio de directiva y marque cualquier vínculo superior como Sin utilizar. Las redes de vSAN volverán a la normalidad cuando finalice esta tarea. Utilice el servicio de estado de vSAN para comprobar que todo funciona correctamente.

---




# Migrar red de máquina virtual

La tarea final necesaria para migrar la red desde un vSwitch estándar a un vSwitch distribuido es migrar la red de máquina virtual.

Para administrar redes de host:

1 Haga clic con el botón derecho en el vDS y seleccione el menú **Agregar y administrar hosts**.

2 Seleccione todos los hosts del clúster para migrar las redes de máquinas virtuales de todos los hosts al vSwitch distribuido.

No mueva ningún vínculo superior. Sin embargo, si la red de máquina virtual de los hosts utiliza un vínculo superior diferente, migre el vínculo superior desde el vSwitch estándar.

3 Seleccione las máquinas virtuales que desea migrar desde una red de máquina virtual en el vSwitch estándar al grupo de puertos distribuidos de la máquina virtual en el vSwitch distribuido. Haga clic en **Asignar grupo de puertos** y seleccione el grupo de puertos distribuidos.

4 Revise los cambios y haga clic en **Finalizar**. En este ejemplo, se va a migrar a las máquinas virtuales. Las plantillas utilizadas por la red de máquina virtual del vSwitch estándar original deben convertirse en máquinas virtuales y editarse. El nuevo grupo de puertos distribuidos de las máquinas virtuales se debe seleccionar como red. Este paso no se puede lograr mediante el asistente de migración.

Dado que el vSwitch estándar ya no tiene ningún vínculo superior ni ningún grupo de puertos, se puede eliminar de forma segura.

Esto completará la migración de un conmutador estándar de vSphere a un vSphere Distributed Switch.

# Resumen de la lista de comprobación para redes de vSAN

17

Utilice el resumen de la lista de comprobación para comprobar los requisitos de su red de vSAN.

- Compruebe si utiliza una NIC de 10 GB compartida o una NIC de 1 GB dedicada. Los clústeres basados íntegramente en tecnología Flash requieren NIC de 10 GB.
- Compruebe que las conexiones de formación de equipos de NIC redundantes estén configuradas.
- Compruebe que el control de flujo está habilitado en las NIC del host ESXi.
- Compruebe que el puerto de VMkernel para el tráfico de redes de vSAN esté configurado en cada host.
- Compruebe que la VLAN, la MTU y la subred son idénticas en todas las interfaces.
- Compruebe que puede ejecutar **`vmkping`** correctamente entre todos los hosts. Utilice el servicio de estado para verificar el estado.
- Si utiliza tramas gigantes, compruebe que puede ejecutar **`vmkping`** correctamente con paquetes de tamaño 9000 entre todos los hosts. Utilice el servicio de estado para verificar el estado.
- Si la versión de vSAN es anterior a la 6.6, compruebe si la multidifusión está habilitada en la red.
- Si la versión de vSAN es anterior a la 6.6 y hay varios clústeres de vSAN en la misma red, configure la multidifusión para que utilice direcciones de multidifusión únicas.
- Si la versión de vSAN es anterior a la 6.6 y abarca varios conmutadores, compruebe que la multidifusión está configurada en todos los conmutadores.
- Si la versión de vSAN es anterior a la 6.6 y está enrutada, compruebe que PIM está configurado para permitir el enrutamiento de multidifusión.
- Asegúrese de que el conmutador físico pueda cumplir con los requisitos de vSAN (multidifusión, control de flujo e interoperabilidad de funciones).
- Compruebe que la red no tenga problemas de rendimiento, como un exceso de paquetes descartados o pausas de tramas.
- Verifique que los límites de red estén dentro de los márgenes aceptables.

- Pruebe el rendimiento de la red de vSAN con **iperf** y compruebe que cumple con las expectativas.